TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 29 août 2000 (29.08.00)	
Demande internationale no PCT/FR00/00189	**Référence du dossier du déposant ou du mandataire** 5971.WO
Date du dépôt international (jour/mois/année) 27 janvier 2000 (27.01.00)	**Date de priorité** (jour/mois/année) 27 janvier 1999 (27.01.99)
Déposant GUILLOU, Louis etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

19 juillet 2000 (19.07.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Diana Nissen

no de téléphone: (41-22) 338.83.38

Expéditeur: L'ADMINISTRATION CHARGEE DE L'EXAMEN PRELIMINAIRE INTERNATIONAL

05 AVR 2001

Destinataire:

VIDON, PATRICE
Cabinet Patrice VIDON
Immeuble Germanium
80 Avenue des Buttes de Coësmes
35700 Rennes
FRANCE

COPIE

PCT

NOTIFICATION DE TRANSMISSION DU RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(règle 71.1 du PCT)

Date d'expédition *(jour/mois/année)* 03.04.2001	
Référence du dossier du déposant ou du mandataire: 5971.WO	**NOTIFICATION IMPORTANTE**

Demande internationale No.	Date du dépot international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR00/00189	27/01/2000	27/01/1999

Déposant: FRANCE TELECOM et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. **RAPPEL**

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Losrqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international
Office européen des brevets
D-80298 Munich
Tél. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Fonctionnaire autorisé
Barrio Baranano, A
Tél. +49 89 2399-8621

TRAI DE COOPERATION EN MATIER E BREVETS

Expéditeur : L'ADMINISTRATION CHARGEE DE LA RECHERCHE INTERNATIONALE

PCT

4 AVR. 2000

Destinataire

Cabinet Patrice VIDON
A l'att. de VIDON, PATRICE
Immeuble Germanium
80 Avenue des Buttes de Coësmes
F-35700 Rennes
FRANCE

NOTIFICATION DE TRANSMISSION DU RAPPORT DE RECHERCHE INTERNATIONALE OU DE LA DECLARATION

(règle 44.1 du PCT)

Référence du dossier du déposant ou du mandataire 5971.WO (LB)	Date d'expédition *(jour/mois/année)* 19/04/2000
Demande internationale n° PCT/FR 00/00189	**POUR SUITE A DONNER** voir les paragraphes 1 et 4 ci-après
Déposant FRANCE TELECOM et al.	Date du dépôt international *(jour/mois/année)* 27/01/2000

1. [X] Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

Dépôt de modifications et d'une déclaration selon l'article 19 :
Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.

Où? Directement auprès du Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse
n° de télécopieur: (41-22)740.14.35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. [ ] Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2)a), est transmise ci-joint.

3. [ ] **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

[ ] la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

[ ] la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:

Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90*bis*.1 et 90*bis*.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).

Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Hans Pettersson

NOTES RELATIVES AU FORMULAIRE PCT/RO/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand? Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment? Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

i) la revendication n'est pas modifiée;

ii) la revendication est supprimée;

iii) la revendication est nouvelle;

iv) la revendication remplace une ou plusieurs revendications telles que déposées;

v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."

2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."

3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15,16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."

4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendiations 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demandeinternationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)"

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationalelors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

TRAITE D' 'OOPERATION EN MATIERE DE EVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 5971.WO	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 00189	Date du dépôt international *(jour/mois/année)* 27/01/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 27/01/1999
Déposant FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé**,

[ ] le texte est approuvé tel qu'il a été remis par le déposant

[X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° _____

[ ] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

Abrégé

La preuve est établie au moyen des paramètres suivants:

- un module public n constitué par le produit de f facteurs premiers p_i, f>2,
- un exposant public v,
- m nombres de base g_i, m>1.

Les nombres de base g_i sont tels que les deux équations:

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n, et tel que l'équation

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n dans le cas. où l'exposant public v est de la forme

$$v = 2^k$$

où k est un paramètre de sécurité.

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande colonne 2, ligne 40 -colonne 3, ligne 50	1,6,7
X	EP 0 381 523 A (TOKYO SHIBAURA ELECTRIC CO) 8 août 1990 (1990-08-08) page 2, colonne 25, ligne 3 -page 7	1,5

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 mars 2000	19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Masche, C

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992
EP 0381523 A	08-08-1990	JP 2204768 A	14-08-1990
		JP 3053367 A	07-03-1991
		US 5046094 A	03-09-1991
		JP 3073990 A	28-03-1991
		JP 3072737 A	27-03-1991

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 5971.WO	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00189	Date du dépot international *(jour/mois/année)* 27/01/2000	Date de priorité *(jour/mois/année)* 27/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 8 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
19/07/2000	03.04.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00189

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-36	version initiale				

Revendications, N°:

13	version initiale				
1-12	reçue(s) le	10/01/2001	avec la lettre du	09/01/2001	

Dessins, feuilles:

1/4-4/4	version initiale				

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   - ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   - ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   - ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   - ☐ contenu dans la demande internationale, sous forme écrite.
   - ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   - ☐ remis ultérieurement à l'administration, sous forme écrite.
   - ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   - ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   - ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☒ des revendications, n°s : 13

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-12
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-12
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-12
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) permettant de produire les facteurs premiers dont le produit constitue un module public nécessaire à la mise en oeuvre d'un protocole destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité. Elle concerne aussi l'utilisation (revendication 10) du procédé de production des facteurs premiers dans un tel protocole.

Etat de la technique:

D1 = EP-A-0 311 470 décrit un tel protocole selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA ; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : "Voici mon identité ; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le protocole d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques dans le protocole selon D1 entraîne des temps de calculs importants.

Invention:

Le procédé selon la revendication 1 permet la production de facteurs premiers particuliers, respectant les conditions mentionnées dans la revendication, dont le produit constitue un module public n. Ce module public n est utilisé dans un protocole d'authentification défini dans la revendication 10.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les caractéristiques de détermination des facteurs premiers telles que définies dans la revendication 1. De plus ces facteurs premiers permettent le calcule d'un module public n utilisable dans un protocole d'authentification évitant les inconvénients du protocole selon D1. L'objet de la revendication 1 implique par conséquent une activité inventive (article 33(3) PCT).

La revendication 10 concerne un protocole d'authentification utilisant un module public n constitué par le produit de facteurs premiers déterminés par le procédé selon la revendication 1. Elle remplit donc de ce fait les conditions de l'article 33 PCT.

Les revendications 2 à 9 et 11 à 12 dépendent respectivement des revendications 1 et 10 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII
Irrégularités dans la demande internationale

Les demandes pendantes évoquées à la page 36 de la description ne sont pas identifiées par leurs numéros de demande ou de publication (Directives PCT, II 4.17).

Revendications

1. Procédé permettant de produire les f facteurs premiers $p_1, p_2, \ldots p_f$ d'un protocole destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message M associé à cette entité,

au moyen d'un module public n constitué par le produit desdits f facteurs premiers $p_1, p_2, \ldots p_f$, f étant supérieur ou égal à 2, ou au moyen des f facteurs premiers ;

ledit procédé comprenant l'étape de produire lesdits f facteurs premiers $p_1, p_2, \ldots p_f$, en respectant les conditions suivantes :

- aucune des deux équations (1) et (2) :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'a de solution en x dans l'anneau des entiers modulo n,

- l'équation (3):

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n ;

$g_1, g_2, \ldots g_m$ désignant m nombres de base entiers, distincts, m étant supérieur ou égal à 1 ;

v désignant un exposant public de la forme :

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 ;

ledit procédé comprenant l'étape de choisir en premier :

- le paramètre de sécurité k
- les m nombres de base $g_1, g_2, \ldots g_m$,
- la taille du module n,
- la taille des f facteurs premiers $p_1, p_2, \ldots p_f$.

2. Procédé selon la revendication 1 tel que les m nombres de base $g_1, g_2, \ldots g_m$, sont choisis au moins en partie parmi les premiers nombres

entiers.

3. Procédé selon l'une quelconque des revendications 1 ou 2, tel que le paramètre de sécurité k est un petit nombre entier, notamment inférieur à 100.

4. Procédé selon l'une quelconque des revendications 1 à 3, tel que la taille du module n est supérieure à plusieurs centaines de bits.

5. Procédé selon l'une quelconque des revendications 1 à 4, tel que les f facteurs premiers p_1, p_2, ... p_f ont une taille voisine de la taille du module n divisé par le nombre f de facteurs.

6. Procédé selon l'une quelconque des revendications 1 à 5, tel que parmi les f facteurs premiers p_1, p_2, ... p_f

- on choisit un nombre e de facteurs premiers congrus à 1 modulo 4, e pouvant être nul (dans le cas où e est nul le module n sera ci-après qualifié de module basique, dans le cas où $e > 0$ le module n sera ci-après qualifié de module mixte),

- les f-e autres facteurs premiers sont choisis congrus à 3 modulo 4, f-e étant au moins égal à 2.

7. Procédé selon la revendication 6 tel que pour produire les f-e facteurs premiers p_1, p_2, ... p_{f-e} congrus à 3 modulo 4,
on met en oeuvre les étapes suivantes :

- on choisit le premier facteur premier p_1 congru à 3 modulo 4,

- on choisit le deuxième facteur premier p_2 tel que p_2 soit complémentaire de p_1 par rapport au nombre de base g_1,

- on choisit le facteur p_{i+1} en procédant comme suit en distinguant deux cas :

(1) Cas où $i > m$

- on choisit le facteur p_{i+1} congru à 3 modulo 4,

(2) Cas où $i \leq m$

- on calcule le profil ($Profil_i(g_i)$) de g_i par rapport aux i

premiers facteurs premiers p_i,

◦ si le $\mathbf{Profil}_i(g_i)$ est plat, on choisit le facteur p_{i+1} tel que p_{i+1} soit complémentaire de p_1 par rapport à g_i,

◦ sinon, on choisit parmi les i-1 nombres de bases $g_1, g_2, \ldots g_{i-1}$ et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé g, tel que $\mathbf{Profil}_i(g) = \mathbf{Profil}_i(g_i)$, on choisit ensuite p_{i+1} tel que $\mathbf{Profil}_{i+1}(g_i) \neq \mathbf{Profil}_{i+1}(g)$,

(les expressions "complémentaire", "profil", "profil plat" ayant le sens défini dans la description).

8. Procédé selon la revendication 8 tel que pour choisir le dernier facteur premier p_{f-e} on procède comme suit, en distinguant trois cas :

(1) Cas où f-e-1 > m

◦ on choisit p_{f-e} congru à 3 modulo 4,

(2) Cas où f-e-1 = m

◦ on calcule $\mathbf{Profil}_{f-e-1}(g_m)$ par rapport aux f-e-1 premiers facteurs premiers, de p_1 à p_{f-e-1},

◦ ◦ si $\mathbf{Profil}_{f-e-1}(g_m)$ est plat, on choisit p_{f-e-1} tel qu'il soit complémentaire de p_1 par rapport à g_m ,

◦ ◦ sinon,

◦ ◦ ◦ on choisit parmi les m-1 nombres de bases de g_1 à g_{m-1} et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé g, tel que $\mathbf{Profil}_i(g) = \mathbf{Profil}_i(g_i)$, puis

◦ ◦ ◦ on choisit ensuite p_{f-e} tel que $\mathbf{Profil}_{f-e}(g) \neq \mathbf{Profil}_{f-e}(g_m)$,

(3) Cas où f-e-1 < m

◦ on choisit p_{f-e} tel que les deux conditions suivantes soient satisfaites :

(3.1) Première condition,

◦ on calcule $\mathbf{Profil}_{f-e-1}(g_{f-e-1})$ par rapport aux f-e-1 premiers

facteurs premiers, de p_1 à p_{f-e-1},

° ° si $\mathbf{Profil}_{f-e-1}(g_{f-e-1})$ est plat, on choisit p_{f-e} tel qu'il satisfasse à la première condition d'être complémentaire de p_1 par rapport à g_{f-e-1},

° ° sinon,

° ° ° on choisit parmi les f-e-1 nombres de bases de g_1 à g_{m-1} et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé g, tel que $\mathbf{Profil}_i(g) = \mathbf{Profil}_{f-e-1}(g_{f-e-1})$, puis

° ° ° on choisit ensuite p_{f-e} tel qu'il satisfasse à la première condition d'être tel que $\mathbf{Profil}_{f-e}(g) \neq \mathbf{Profil}_{f-e}(g_m)$,

(3.2) Deuxième condition,

° on sélectionne parmi l'ensemble des derniers nombres de bases de g_{f-e} à g_m ceux dont le profil $\mathbf{Profil}_{f-e-1}(g_i)$ est plat, puis

° on choisit p_{f-e} tel qu'il satisfasse à la deuxième condition d'être complémentaire de p_1 par rapport à chacun des nombres de bases ainsi sélectionnés.

9 Procédé selon les revendications 7 ou 8 tel que pour produire les e facteurs premiers congrus à 1 modulo 4, on évalue chaque candidat facteur premier p , de p_{f-e} à p_f , en lui faisant subir les deux tests successifs suivants :

(1) Premier test

- on calcule le symbole de Legendre de chaque nombre de base g_i , de g_1 à g_m , par rapport au facteur premier p candidat,

° si le symbole de Legendre est égal à -1, on rejette le candidat p,

° si le symbole de Legendre est égal à +1, on poursuit l'évaluation du candidat p en passant au nombre de base suivant, puis lorsque le dernier nombre de base a été pris en compte on passe au deuxième test,

(2) Deuxième test,

- on calcule un nombre entier t tel que p-1 est divisible par 2^t mais pas par 2^{t+1}, puis

- on calcule un entier s tel que $s = (p-1+2^t)/2^{t+1}$,

- on applique la clé $\langle s, p \rangle$ à chaque valeur publique G_i pour obtenir un résultat r

$$r \equiv G_i^{\,s} \bmod p$$

◦ si r est égal à g_i ou $-g_i$, on poursuit le deuxième test en passant à la valeur publique G_{i+1} suivante,

◦ si r est différent de g_i ou $-g_i$, on calcule un facteur u en appliquant l'algorithme suivant :

◦◦ l'algorithme consiste à répéter la séquence suivante pour un indice ii allant de 1 à t-2 :

◦◦ l'algorithme met en oeuvre deux variables : w initialisée par r et $jj = 2^{ii}$ prenant des valeurs allant de 2 à 2^{t-2}, ainsi qu'un nombre b obtenu par l'application de la clé $\langle (p-1)/2^t, p \rangle$ à un résidu non quadratique de CG(p), puis, on itère les étapes 1 et 2 suivantes,

◦◦◦ étape 1 : on calcule $w^2/G_i \pmod p$,

◦◦◦ étape 2 : on élève le résultat à la puissance 2^{t-ii-1}

◦◦◦◦ si on obtient +1, on poursuit le deuxième test en passant à la valeur publique G_{i+1} suivante,

◦◦◦◦ si on obtient -1, on calcule $jj = 2^{ii}$, puis on remplace w par $w.b^{jj} \pmod p$, puis on poursuit l'algorithme pour la valeur suivante de l'indice ii,

◦◦ à l'issue de l'algorithme, la valeur figurant dans la variable jj permet de calculer un nombre entier u par la relation $jj = 2^{t-u}$, puis on calcule l'expression t-u, deux cas se présentent :

◦◦◦ si $t-u < k$, on rejette le candidat p

◦◦◦ si $t-u \geq k$, on continue l'évaluation du candidat p en poursuivant le deuxième test en passant à la valeur publique G_{i+1} suivante,

le candidat **p** est accepté comme facteur premier congru à 1 modulo 4 si à l'issue du deuxième test, pour toutes les **m** valeurs publiques G_i , il n'a pas été rejeté.

10. Protocole faisant application du procédé selon l'une quelconque des revendications 1 à 9 ; ledit protocole étant destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message M associé à cette entité,

au moyen de **m** couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, ou des paramètres dérivés de ceux-ci ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i . Q_i^v \equiv 1 \ . \mathbf{mod}\ n \text{ ou } G_i \equiv Q_i^v \mathbf{mod}\ n ;$$

ladite valeur publique G_i étant le carré g_i^2 du nombre de base g_i inférieur aux **f** facteurs premiers $p_1, p_2, \ldots p_f$;

ledit protocole mettant en œuvre selon les étapes suivantes une entité appelée témoin disposant des **f** facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public **n** et/ou des **m** valeurs privées Q_i et/ou des **f.m** composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) des valeurs privées Q_i et de l'exposant public **v** ;

- le témoin calcule des engagements $\mathbb{R}$ dans l'anneau des entiers modulo **n** ; chaque engagement étant calculé :

  ◦ soit en effectuant des opérations du type

$$\mathbb{R} \equiv r^v \mathbf{mod}\ n$$

où **r** est un aléa tel que $0 < r < n$,

  ◦ soit

    ◦◦ en effectuant des opérations du type

$$R_i \equiv r_i^v \mathbf{mod}\ p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$,

°° puis en appliquant la méthode des restes chinois ;

- le témoin reçoit un ou plusieurs défis **d** ; chaque défi **d** comportant **m** entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi **d** une réponse $\mathbb{D}$,

° soit en effectuant des opérations du type :

$$\mathbb{D} \equiv r \cdot Q_1^{\,d1} \cdot Q_2^{\,d2} \cdot \ldots Q_m^{\,dm} \bmod n$$

° soit

°° en effectuant des opérations du type :

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i$$

°° puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses $\mathbb{D}$ que de défis **d** que d'engagements $\mathbb{R}$, chaque groupe de nombres $\mathbb{R}$, **d**, $\mathbb{D}$ constituant un triplet noté $\{\mathbb{R}, d, \mathbb{D}\}$.

11. Procédé selon la revendication 10 tel que pour mettre en oeuvre les couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, on utilise les facteurs premiers $p_1, p_2, \ldots p_f$ et/ou les paramètres des restes chinois, les nombres de bases $g_1, g_2, \ldots g_m$ et/ou les valeurs publiques $G_1, G_2, \ldots G_m$ pour calculer :

- soit les valeurs privées $Q_1, Q_2, \ldots Q_m$ en extrayant une **k ième** racine carrée modulo **n** de G_i , ou en prenant l'inverse d'une **k ième** racine carrée modulo **n** de G_i ,

- soit les **f.m** composantes privées $Q_{i,j}$ des valeurs privées $Q_1, Q_2, \ldots Q_m$, telles que $Q_{i,j} \equiv Q_i \pmod{p_j}$,

12 Procédé selon la revendication 11 tel que pour calculer les **f.m** composantes privées $Q_{i,j}$ des valeurs privées $Q_1, Q_2, \ldots Q_m$:

- on applique la clé $\langle s, p_j \rangle$ pour calculer **z** tel que

$$z \equiv G_i^{\,s} \pmod{p_j}$$

- on utilise les valeurs **t** et **u**

° calculées comme indiqué ci-dessus dans le cas où p_j est congru

à 1 modulo 4 et

◦ prises respectivement égales à 1 (t=1) et 0 (u=0) dans le cas où p_j est congru à 3 modulo 4,

◦ ◦ si **u** est nul on considère l'ensemble des nombres zz tels que :

◦ ◦ ◦ zz soit égale à z ou tel que

◦ ◦ ◦ zz soit égale au produit (mod p_j) de z par chacune des 2^{ii-t} racines 2^{ii}ièmes primitives de l'unité, ii allant de 1 à min(k,t) ,

◦ ◦ si **u** est positif on considère l'ensemble des nombres zz tels que zz soit égale au produit (mod p_j) de za par chacune des 2^k racines 2^k ièmes de l'unité, za désignant la valeur de la variable w à l'issue de l'algorithme mis en oeuvre dans la revendication 10,

- on en déduit au moins une valeur de la composante $Q_{i,j}$ elle est égale à zz lorsque l'équation $G_i \equiv Q_i^v$ **mod n** est utilisée ou bien elle est égale à l'inverse de zz modulo p_j de zz lorsque l'équation $G_i . Q_i^v \equiv 1 .$ **mod n** est utilisée.

03/869960 Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 5971.WO	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00189	International filing date (*day/month/year*) 27 January 2000 (27.01.00)	Priority date (*day/month/year*) 27 January 1999 (27.01.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant FRANCE TELECOM		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 19 July 2000 (19.07.00)	Date of completion of this report 03 April 2001 (03.04.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00189

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-36, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

☒ the claims:

pages 13, as originally filed

pages _____, as amended (together with any statement under Article 19

pages _____, filed with the demand

pages 1-12, filed with the letter of 10 January 2001 (10.01.2001)

☒ the drawings:

pages 1/4-4/4, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☒ the claims, Nos. 13

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		NO
Inventive step (IS)	Claims	1-12	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations

The invention relates to a method (Claim 1) for producing prime factors whereof the product constitutes a public module necessary for implementing a protocol designed to prove the authenticity of an entity, and/or the integrity of a message associated with said entity, to a verifier entity. The invention also relates to the use (Claim 10) of the method for producing prime factors in such a protocol.

Prior art:

D1 (EP-A-0 311 470) describes such a protocol according to which an entity known as "trusted authority" attributes an identity to each so-called "witness" entity, and calculates the RSA signature thereof. During a customization process, the trusted authority gives the witness an identity and signature. Subsequently, the witness states: "This is my identity; I know the RSA signature thereof". The witness proves that it knows the RSA signature of its identity without revealing said signature. The public RSA verification key distributed by the trusted authority enables a so-called "verifier" entity verifies that the RSA signature matches the stated identity, without the signature being disclosed to said

entity. The mechanisms using this protocol operate "without knowledge transfer": the witness does not know the private RSA key with which the trusted authority signs a large number of identities.

Problem:

The use of RSA technology makes the authentication protocol sensitive to "multiplicative" attacks. Furthermore, the workload associated with the arithmetic operations in the protocol according to D1 leads to long calculation times.

Invention:

The method according to Claim 1 produces particular prime factors, the product of which constitutes a public module n, while respecting the conditions mentioned in the claim. Said public module n is used in an authentication protocol defined in Claim 10.

None of the documents cited in the international search report discloses or suggests the features for determining prime factors such as those defined in Claim 1. Moreover, said prime factors lead to the calculation of a public module n that can be used in an authentication protocol that avoids the disadvantages of the protocol according to D1. The subject matter of Claim 1 therefore involves an inventive step (PCT Article 33(3)).

Claim 10 relates to an authentication protocol that uses a public module n consisting of the product of prime factors predetermined by the method according to Claim 1. Said claim therefore meets the requirements of PCT Article 33.

Claims 2 to 9 and 11 to 12 are dependent on Claims 1 and 10, respectively, and therefore also meet, as such, the PCT requirements of novelty and inventive step.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The pending applications set forth on page 36 of the description have not been identified by their application or publication numbers (PCT Examination Guidelines, II 4.17).

TRAITE D OOPERATION EN MATIERE DE . .EVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
5971.WO		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 00189	27/01/2000	27/01/1999
Déposant		
FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé**,

   [ ] le texte est approuvé tel qu'il a été remis par le déposant

   [X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des **dessins** à publier avec l'abrégé est la Figure n° _____

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

Abrégé

La preuve est établie au moyen des paramètres suivants:

- un module public n constitué par le produit de f facteurs premiers p_i, f>2.
- un exposant public v,
- m nombres de base g_i, m>1.

Les nombres de base g_i sont tels que les deux équations:

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n, et tel que l'équation

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n dans le cas, où l'exposant public v est de la forme

$$v = 2^k$$

où k est un paramètre de sécurité.

RAPPORT DE RECHERCHE INTERNATIONALE

mande internationale No

PCT/FR 00/00189

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande colonne 2, ligne 40 -colonne 3, ligne 50	1,6,7
X	EP 0 381 523 A (TOKYO SHIBAURA ELECTRIC CO) 8 août 1990 (1990-08-08) page 2, colonne 25, ligne 3 -page 7	1,5

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 mars 2000	19/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Masche, C

Renseignements relatifs a mbres de familles de brevets

mande internationale no

PCT/FR 00/00189

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992
EP 0381523 A	08-08-1990	JP 2204768 A	14-08-1990
		JP 3053367 A	07-03-1991
		US 5046094 A	03-09-1991
		JP 3073990 A	28-03-1991
		JP 3072737 A	27-03-1991

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 April 1989 (1989-04-12) cited in the application column 2, line 40 -column 3, line 50	1,6,7
X	EP 0 381 523 A (TOKYO SHIBAURA ELECTRIC CO) 8 August 1990 (1990-08-08) page 2, column 25, line 3 -page 7	1,5

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 March 2000	19/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992
EP 0381523 A	08-08-1990	JP 2204768 A	14-08-1990
		JP 3053367 A	07-03-1991
		US 5046094 A	03-09-1991
		JP 3073990 A	28-03-1991
		JP 3072737 A	27-03-1991

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

1ST

Référence du dossier du déposant ou du mandataire 5971.WO	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00189	Date du dépot international *(jour/mois/année)* 27/01/2000	Date de priorité *(jour/mois/année)* 27/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 8 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
19/07/2000	03.04.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-36	version initiale			

Revendications, N°:

13	version initiale			
1-12	reçue(s) le	10/01/2001	avec la lettre du	09/01/2001

Dessins, feuilles:

1/4-4/4	version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

☐ de la description, pages :
☒ des revendications, n^os^ : 13
☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-12
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-12
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-12
	Non :	Revendications	

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) permettant de produire les facteurs premiers dont le produit constitue un module public nécessaire à la mise en oeuvre d'un protocole destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité. Elle concerne aussi l'utilisation (revendication 10) du procédé de production des facteurs premiers dans un tel protocole.

Etat de la technique:

D1 = EP-A-0 311 470 décrit un tel protocole selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA ; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : "Voici mon identité ; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le protocole d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques dans le protocole selon D1 entraîne des temps de calculs importants.

Invention:

Le procédé selon la revendication 1 permet la production de facteurs premiers particuliers, respectant les conditions mentionnées dans la revendication, dont le produit constitue un module public n. Ce module public n est utilisé dans un protocole d'authentification défini dans la revendication 10.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les caractéristiques de détermination des facteurs premiers telles que définies dans la revendication 1. De plus ces facteurs premiers permettent le calcule d'un module public n utilisable dans un protocole d'authentification évitant les inconvénients du protocole selon D1. L'objet de la revendication 1 implique par conséquent une activité inventive (article 33(3) PCT).

La revendication 10 concerne un protocole d'authentification utilisant un module public n constitué par le produit de facteurs premiers déterminés par le procédé selon la revendication 1. Elle remplit donc de ce fait les conditions de l'article 33 PCT.

Les revendications 2 à 9 et 11 à 12 dépendent respectivement des revendications 1 et 10 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII

Irrégularités dans la demande internationale

Les demandes pendantes évoquées à la page 36 de la description ne sont pas identifiées par leurs numéros de demande ou de publication (Directives PCT, II 4.17).

Revendications

1. Procédé permettant de produire les f facteurs premiers $p_1, p_2, \ldots p_f$ d'un protocole destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message M associé à cette entité,

au moyen d'un module public n constitué par le produit desdits f facteurs premiers $p_1, p_2, \ldots p_f$, f étant supérieur ou égal à 2, ou au moyen des f facteurs premiers ;

ledit procédé comprenant l'étape de produire lesdits f facteurs premiers $p_1, p_2, \ldots p_f$, en respectant les conditions suivantes :

- aucune des deux équations (1) et (2) :

$$x^2 \equiv g_i \bmod n \quad \text{et} \quad x^2 \equiv -g_i \bmod n$$

n'a de solution en x dans l'anneau des entiers modulo n,

- l'équation (3):

$$x^v \equiv g_i^2 \bmod n$$

a des solutions en x dans l'anneau des entiers modulo n ;

$g_1, g_2, \ldots g_m$ désignant m nombres de base entiers, distincts, m étant supérieur ou égal à 1 ;

v désignant un exposant public de la forme :

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1 ;

ledit procédé comprenant l'étape de choisir en premier :

- le paramètre de sécurité k
- les m nombres de base $g_1, g_2, \ldots g_m$,
- la taille du module n,
- la taille des f facteurs premiers $p_1, p_2, \ldots p_f$.

2. Procédé selon la revendication 1 tel que les m nombres de base $g_1, g_2, \ldots g_m$, sont choisis au moins en partie parmi les premiers nombres

entiers.

3. Procédé selon l'une quelconque des revendications 1 ou 2, tel que le paramètre de sécurité k est un petit nombre entier, notamment inférieur à 100.

4. Procédé selon l'une quelconque des revendications 1 à 3, tel que la taille du module n est supérieure à plusieurs centaines de bits.

5. Procédé selon l'une quelconque des revendications 1 à 4, tel que les f facteurs premiers p_1, p_2, ... p_f ont une taille voisine de la taille du module n divisé par le nombre f de facteurs.

6. Procédé selon l'une quelconque des revendications 1 à 5, tel que parmi les f facteurs premiers p_1, p_2, ... p_f

- on choisit un nombre e de facteurs premiers congrus à 1 modulo 4, e pouvant être nul (dans le cas où e est nul le module n sera ci-après qualifié de module basique, dans le cas où $e > 0$ le module n sera ci-après qualifié de module mixte),

- les f-e autres facteurs premiers sont choisis congrus à 3 modulo 4, f-e étant au moins égal à 2.

7. Procédé selon la revendication 6 tel que pour produire les f-e facteurs premiers p_1, p_2, ... p_{f-e} congrus à 3 modulo 4,

on met en oeuvre les étapes suivantes :

- on choisit le premier facteur premier p_1 congru à 3 modulo 4,

- on choisit le deuxième facteur premier p_2 tel que p_2 soit complémentaire de p_1 par rapport au nombre de base g_1,

- on choisit le facteur p_{i+1} en procédant comme suit en distinguant deux cas :

(1) Cas où $i > m$

- on choisit le facteur p_{i+1} congru à 3 modulo 4,

(2) Cas où $i \leq m$

- on calcule le profil ($\mathbf{Profil}_i(g_i)$) de g_i par rapport aux i

premiers facteurs premiers p_i,

◦ si le $\mathbb{P}\mathbf{rofil}_i(g_i)$ est plat, on choisit le facteur p_{i+1} tel que p_{i+1} soit complémentaire de p_1 par rapport à g_i,

◦ sinon, on choisit parmi les i-1 nombres de bases $g_1, g_2, \ldots g_{i-1}$ et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé g, tel que $\mathbb{P}\mathbf{rofil}_i(g) = \mathbb{P}\mathbf{rofil}_i(g_i)$, on choisit ensuite p_{i+1} tel que $\mathbb{P}\mathbf{rofil}_{i+1}(g_i) \neq \mathbb{P}\mathbf{rofil}_{i+1}(g)$,

(les expressions "complémentaire", "profil", "profil plat" ayant le sens défini dans la description).

8. Procédé selon la revendication 8 tel que pour choisir le dernier facteur premier p_{f-e} on procède comme suit, en distinguant trois cas :

(1) Cas où f-e-1 > m

◦ on choisit p_{f-e} congru à 3 modulo 4,

(2) Cas où f-e-1 = m

◦ on calcule $\mathbb{P}\mathbf{rofil}_{f-e-1}(g_m)$ par rapport aux f-e-1 premiers facteurs premiers, de p_1 à p_{f-e-1},

◦ ◦ si $\mathbb{P}\mathbf{rofil}_{f-e-1}(g_m)$ est plat, on choisit p_{f-e-1} tel qu'il soit complémentaire de p_1 par rapport à g_m ,

◦ ◦ sinon,

◦ ◦ ◦ on choisit parmi les m-1 nombres de bases de g_1 à g_{m-1} et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé g, tel que $\mathbb{P}\mathbf{rofil}_i(g) = \mathbb{P}\mathbf{rofil}_i(g_i)$, puis

◦ ◦ ◦ on choisit ensuite p_{f-e} tel que $\mathbb{P}\mathbf{rofil}_{f-e}(g) \neq \mathbb{P}\mathbf{rofil}_{f-e}(g_m)$,

(3) Cas où f-e-1 < m

◦ on choisit p_{f-e} tel que les deux conditions suivantes soient satisfaites :

(3.1) Première condition,

◦ on calcule $\mathbb{P}\mathbf{rofil}_{f-e-1}(g_{f-e-1})$ par rapport aux f-e-1 premiers

facteurs premiers, de p_1 à p_{f-e-1},

◦ ◦ si $\mathbb{P}rofil_{f-e-1}(g_{f-e-1})$ est plat, on choisit p_{f-e} tel qu'il satisfasse à la première condition d'être complémentaire de p_1 par rapport à g_{f-e-1},

◦ ◦ sinon,

◦ ◦ ◦ on choisit parmi les f-e-1 nombres de bases de g_1 à g_{m-1} et toutes leurs combinaisons multiplicatives le nombre, ci-après dénommé g, tel que $\mathbb{P}rofil_i(g) = \mathbb{P}rofil_{f-e-1}(g_{f-e-1})$, puis

◦ ◦ ◦ on choisit ensuite p_{f-e} tel qu'il satisfasse à la première condition d'être tel que $\mathbb{P}rofil_{f-e}(g) \neq \mathbb{P}rofil_{f-e}(g_m)$,

(3.2) Deuxième condition,

◦ on sélectionne parmi l'ensemble des derniers nombres de bases de g_{f-e} à g_m ceux dont le profil $\mathbb{P}rofil_{f-e-1}(g_i)$ est plat, puis

◦ on choisit p_{f-e} tel qu'il satisfasse à la deuxième condition d'être complémentaire de p_1 par rapport à chacun des nombres de bases ainsi sélectionnés.

9 Procédé selon les revendications 7 ou 8 tel que pour produire les e facteurs premiers congrus à 1 modulo 4, on évalue chaque candidat facteur premier p , de p_{f-e} à p_f , en lui faisant subir les deux tests successifs suivants :

(1) Premier test

- on calcule le symbole de Legendre de chaque nombre de base g_i , de g_1 à g_m , par rapport au facteur premier p candidat,

◦ si le symbole de Legendre est égal à -1, on rejette le candidat p,

◦ si le symbole de Legendre est égal à +1, on poursuit l'évaluation du candidat p en passant au nombre de base suivant, puis lorsque le dernier nombre de base a été pris en compte on passe au deuxième test,

(2) Deuxième test,

- on calcule un nombre entier t tel que p-1 est divisible par 2^t mais pas par 2^{t+1} , puis

- on calcule un entier s tel que $s = (p-1+2^t)/2^{t+1}$,

- on applique la clé $\langle s, p \rangle$ à chaque valeur publique G_i pour obtenir un résultat r

$$r \equiv G_i^{\,s} \bmod p$$

◦ si r est égal à g_i ou - g_i , on poursuit le deuxième test en passant à la valeur publique G_{i+1} suivante,

◦ si r est différent de g_i ou - g_i , on calcule un facteur u en appliquant l'algorithme suivant :

◦ ◦ l'algorithme consiste à répéter la séquence suivante pour un indice ii allant de 1 à t-2 :

◦ ◦ l'algorithme met en oeuvre deux variables : w initialisée par r et $jj = 2^{ii}$ prenant des valeurs allant de 2 à 2^{t-2} , ainsi qu'un nombre b obtenu par l'application de la clé $\langle (p-1)/2^t, p \rangle$ à un résidu non quadratique de CG(p), puis, on itère les étapes 1 et 2 suivantes,

◦ ◦ ◦ étape 1 : on calcule $w^2/G_i \pmod p$,

◦ ◦ ◦ étape 2 : on élève le résultat à la puissance 2^{t-ii-1}

◦ ◦ ◦ ◦ si on obtient +1 , on poursuit le deuxième test en passant à la valeur publique G_{i+1} suivante,

◦ ◦ ◦ ◦ si on obtient -1, on calcule $jj = 2^{ii}$, puis on remplace w par $w.b^{jj} \pmod p$, puis on poursuit l'algorithme pour la valeur suivante de l'indice ii,

◦ ◦ à l'issue de l'algorithme, la valeur figurant dans la variable jj permet de calculer un nombre entier u par la relation $jj = 2^{t-u}$, puis on calcule l'expression t-u, deux cas se présentent :

◦ ◦ ◦ si $t-u < k$, on rejette le candidat p

◦ ◦ ◦ si $t-u \geq k$, on continue l'évaluation du candidat p en poursuivant le deuxième test en passant à la valeur publique G_{i+1} suivante,

le candidat p est accepté comme facteur premier congru à 1 modulo 4 si à l'issue du deuxième test, pour toutes les m valeurs publiques G_i , il n'a pas été rejeté.

10. Protocole faisant application du procédé selon l'une quelconque des revendications 1 à 9 ; ledit protocole étant destiné à prouver à une entité contrôleur,

- l'authenticité d'une entité et/ou
- l'intégrité d'un message M associé à cette entité,

au moyen de m couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, ou des paramètres dérivés de ceux-ci ;

ledit module et lesdites valeurs étant liés par des relations du type :

$$G_i . Q_i^v \equiv 1 \ . \bmod n \text{ ou } G_i \equiv Q_i^{-v} \bmod n ;$$

ladite valeur publique G_i étant le carré g_i^2 du nombre de base g_i inférieur aux f facteurs premiers $p_1, p_2, \ldots p_f$;

ledit protocole mettant en œuvre selon les étapes suivantes une entité appelée témoin disposant des f facteurs premiers p_i et/ou des paramètres des restes chinois des facteurs premiers et/ou du module public n et/ou des m valeurs privées Q_i et/ou des fm composantes $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) des valeurs privées Q_i et de l'exposant public v ;

- le témoin calcule des engagements R dans l'anneau des entiers modulo n ; chaque engagement étant calculé :
  - soit en effectuant des opérations du type

$$R \equiv r^v \bmod n$$

où r est un aléa tel que $0 < r < n$,

  - soit
    - en effectuant des opérations du type

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un aléa associé au nombre premier p_i tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1 , r_2 , \ldots r_f\}$,

°° puis en appliquant la méthode des restes chinois ;

- le témoin reçoit un ou plusieurs défis d ; chaque défi d comportant m entiers d_i ci-après appelés défis élémentaires ; le témoin calcule à partir de chaque défi d une réponse D,

° soit en effectuant des opérations du type :

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

° soit

°° en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

°° puis en appliquant la méthode des restes chinois ;

ledit procédé étant tel qu'il y a autant de réponses D que de défis d que d'engagements R, chaque groupe de nombres R, d, D constituant un triplet noté {R, d, D}.

11. Procédé selon la revendication 10 tel que pour mettre en oeuvre les couples de valeurs privées $Q_1, Q_2, \ldots Q_m$ et publiques $G_1, G_2, \ldots G_m$, on utilise les facteurs premiers $p_1, p_2, \ldots p_f$ et/ou les paramètres des restes chinois, les nombres de bases $g_1, g_2, \ldots g_m$ et/ou les valeurs publiques $G_1, G_2, \ldots G_m$ pour calculer :

- soit les valeurs privées $Q_1, Q_2, \ldots Q_m$ en extrayant une k ième racine carrée modulo n de G_i , ou en prenant l'inverse d'une k ième racine carrée modulo n de G_i ,

- soit les fm composantes privées $Q_{i,j}$ des valeurs privées $Q_1, Q_2, \ldots Q_m$, telles que $Q_{i,j} \equiv Q_i \pmod{p_j}$,

12 Procédé selon la revendication 11 tel que pour calculer les fm composantes privées $Q_{i,j}$ des valeurs privées $Q_1, Q_2, \ldots Q_m$:

- on applique la clé $\langle s, p_j \rangle$ pour calculer z tel que

$$z \equiv G_i^s \pmod{p_j}$$

- on utilise les valeurs t et u

° calculées comme indiqué ci-dessus dans le cas où p_j est congru

à 1 modulo 4 et

◦ prises respectivement égales à 1 (t=1) et 0 (u=0) dans le cas où p_j est congru à 3 modulo 4,

◦ ◦ si u est nul on considère l'ensemble des nombres zz tels que :

◦ ◦ ◦ zz soit égale à z ou tel que

◦ ◦ ◦ zz soit égale au produit (mod p_j) de z par chacune des 2^{ii-t} racines 2^{ii}ièmes primitives de l'unité, ii allant de 1 à min(k,t) ,

◦ ◦ si u est positif on considère l'ensemble des nombres zz tels que zz soit égale au produit (mod p_j) de za par chacune des 2^k racines 2^k ièmes de l'unité, za désignant la valeur de la variable w à l'issue de l'algorithme mis en oeuvre dans la revendication 10,

- on en déduit au moins une valeur de la composante $Q_{i,j}$ elle est égale à zz lorsque l'équation $G_i \equiv Q_i^v \bmod n$ est utilisée ou bien elle est égale à l'inverse de zz modulo p_j de zz lorsque l'équation $G_i . Q_i^v \equiv 1 . \bmod n$ est utilisée.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 792 044 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.08.1997 Bulletin 1997/35

(51) Int. Cl.[6]: **H04L 9/32**

(21) Application number: **97102779.2**

(22) Date of filing: **20.02.1997**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **23.02.1996 JP 62076/96**
06.01.1997 JP 418/97

(71) Applicant: **FUJI XEROX CO., LTD.**
Minato-ku, Tokyo (JP)

(72) Inventors:
- **Shin, Kil-ho**
  Ashigarakami-gun, Kanagawa (JP)
- **Kobayashi, Kenichi**
  Ashigarakami-gun, Kanagawa (JP)
- **Aratani, Toru**
  Ashigarakami-gun, Kanagawa (JP)

(74) Representative: **Hoffmann, Eckart, Dipl.-Ing.**
Patentanwalt,
Bahnhofstrasse 103
82166 Gräfelfing (DE)

(54) Device and method for authenticating user's access rights to resources according to the Challenge-Response principle

(57) The present invention provides a device for authenticating user's access rights to resources, which comprises first memory means 111 for storing challenging data 18, second memory means 115 for storing unique identifying information of the user 116, third memory means 113 for storing proof support information 13 which is a result of executing predetermined computations to the unique identifying information of the user 16 and unique security characteristic information of the device 14, response generation means 116 for generating a response 19 from the challenging data 18 stored in the first memory means 111, the unique identifying information 16 stored in the second memory means 115 and the proof support information 13 stored in the third memory means 113, and verification means 106 for verifying the legitimacy of the response 19 by verifying that the response 19, the challenging data 18 and the unique security characteristic information of the device 14 satisfy a specific predefined relation.

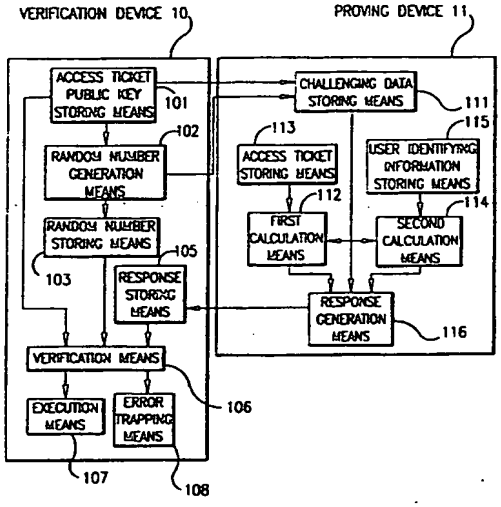


FIG.3

EP 0 792 044 A2

Description

The present invention relates to a device for authenticating user's access rights to resources.

Program execution control technologies are known in the field to which the present invention belongs. The program execution control technologies are technologies to:

1. Embed a routine for user authentication during the use of an application program;
2. Have the routine examine whether the user attempting execution of the application possesses a key for proper authentication; and
3. Continue the program only when the existence of the key for authentication is verified, otherwise to halt execution.

By using these technologies, execution of the application program is enabled only for proper users having the authentication key. The technologies are commercialized in the software marketing field, two examples being SentinelSuperPro (trade mark) from Rainbow Technologies, Inc. and HASP (trade mark) from Aladdin Knowledge Systems, Ltd.

In the use of program execution control technologies, a user who executes software possesses an authentication key as user identification information. The authentication key is a key for encryption and is distributed to the user by a party who allows use of software, a software vender, for example. The authentication key is securely sealed in a memory, or the like, of hardware to prevent duplication, and is delivered to the user using physical means such as the postal service. The user mounts personal computer/workstation using a designated method. When the user starts up the application program and when the execution of the program reaches the user authentication routine, the program communicates with the hardware in which the authentication key of the user is embedded. Based on the results of the communication, the program identifies the authentication key, and moves the execution to the following step upon confirmation of existence of the correct authentication key. If the communication fails and the verification of the existence of the authentication key is not established, the program stops automatically, discontinuing the execution of subsequent steps.

Identification of the authentication key by the user authentication routine is executed according to the following protocol, for example:

1. The user authentication routine generates and transmits an appropriate number to the hardware in which the key is embedded.
2. The hardware in which the key is embedded encrypts the number using the embedded authentication key and transmits it back to the authentication routine.
3. The authentication routine determines whether or not the number transmitted back is the number expected beforehand, or, in other words, the number obtained by encrypting the number with a correct authentication key.
4. If the number transmitted back coincides with the expected number, the execution of the program is continued, otherwise the execution is halted.
5. In this case, communication between the application program and the hardware in which the authentication key is embedded must be different for each execution even if it is between the same location in the same application with the same hardware.

Otherwise, a user who does not possess the correct authentication key may be able to execute the program by recording once the content of communication during the normal execution process, and by responding to the application program according to the recording each time the subsequent program is executed. Such improper execution of the application program by replaying the communication content is called a replay attack.

In order to prevent a replay attack, in general, a random number is generated and used for each communication as the number to be transmitted to the hardware in which the key is embedded.

The present invention has been made in view of the above circumstances and an aspect of the present invention is to provide a device for authenticating user's access rights to resources and its method which set both users and the protecting side such as application providers free from inconveniences caused by handling of large amount of unique information, for example, a lot of authentication keys, and thereby user's access rights are easily and simply authenticated when the execution control of the program, privacy protection of electronic mails, access control of files or computer resources and so forth are carried out.

Additional aspects and advantages of the invention will be set forth in part in the description which follows and in part will be obvious from the description, or may be learned by practice of the invention. The aspects and advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims. It will be understood that each of the features described herein can be taken separately or jointly. To achieve the aspects and in accordance with the purpose of the invention, as embodied and broadly described herein, one aspect of a device for authenticating user's access rights to resources of the present invention comprises first memory means for storing challenging data, second memory means for storing unique identifying information of the user, third memory means for storing proof support information which is a result of executing predetermined computations to the user unique identifying information and unique security characteristic

information of the device, response generation means for generating a response from the challenging data stored in the first memory means, the unique identifying information stored in the second memory means and the proof support information stored in the third memory means, and verification means for verifying the legitimacy of the response by verifying that the response, the challenging data and the unique security characteristic information of the device satisfy a specific predefined relation.

With the above constitution, the unique security characteristic information of the device assigned to the protecting side and the unique identifying information of the user are made to be independent of each other. The information on actual access rights is represented as proof support information (i.e., an access ticket). The user has the user unique identifying information in advance, and on the other hand, a protector, such as a program creator prepares the unique security characteristic information, or the counterpart of the unique security characteristic information in terms of the public key cryptography, independent of the user unique identifying information held by the user. An access ticket is generated based on the user unique identifying information and the unique security characteristic information used in creation of the application program or the like. Access tickets are distributed to the users, whereby authentication of the user's access rights to resources such as execution control can be performed. Thus complexity occurring in the case where both sides of user and protector use the same information for performing authentication can be avoided.

Moreover, in the above constitution, at least the second memory means and the response generation means may be confined in the protect means which prevents any data inside from being observed or being tampered with from the outside. It may also be possible to implement at least the second memory means and the response generation means within a small portable device such as a smart card.

The response generating means may comprise first calculation means and second calculation means, wherein the first calculation means executes predetermined calculations to the user unique identifying information stored in the second memory means and the proof support information stored in the third memory means to obtain the unique security characteristic information as a result, and the second calculation means executes predetermined calculations to the challenging data stored in the first memory means and the unique security characteristic information calculated by the first calculation means to generate the response as a result of calculation.

The above-described response generation means may comprise third calculation means, fourth calculation means and fifth calculation means. The third calculation means executes predetermined calculations to the challenging data stored in the first memory means and the proof support information stored in the third memory means, the fourth calculation means executes predetermined calculations to the challenging data stored in the first memory means and the user unique identifying information stored in the second memory means, and the fifth calculation means executes predetermined calculations to the results of calculation by the third and fourth calculation means, whereby the response is generated. In this case, at least the second memory means and the fourth calculation means can be confined within the protect means which prevents any data inside from being observed or being tampered with from the outside. At least the second memory means and the fourth calculation means may be implemented within a small portable device such as a smart card.

The accompanying drawings, which are incorporated in and constitute a part of this specification illustrate embodiment of the invention and, together with the description, serve to explain the objects, advantages and principles of the invention. In the drawings:

Fig. 1 is a block diagram showing an example of the fundamental constitution of the present invention;
Fig. 2 is a block diagram showing an example of the constitution of the present invention in case that an entire device is implemented within a single PC;
Fig. 3 is a block diagram showing the constitution of a first embodiment of a device for authenticating user's access rights to resources according to the present invention;
Fig. 4 is a flow chart showing functions of means constituting the devices of the first embodiment;
Fig. 5 is a block diagram showing the constitutions of a verification device and a proving device of a second embodiment of the device for authenticating user's access rights to resources according to the present invention;
Fig. 6 is a flow chart showing functions of means constituting the verification device of the second embodiment;
Fig. 7 is a block diagram showing a constitutional example of execution means of the verification means of the second embodiment;
Fig. 8 is a flow chart showing functions of the constitutional example of the execution means shown in Fig. 7;
Fig. 9 is a block diagram showing a second constitutional example of execution means of the verification means of the second embodiment;
Fig. 10 is a flow chart showing functions of the constitutional example of the execution means shown in Fig. 9;
Fig. 11 is a block diagram showing a third constitutional example of execution means of the verification means of the second embodiment;
Fig. 12 is a flow chart showing functions of the constitutional example of the execution means shown in Fig. 11;
Fig. 13 is a block diagram showing a fourth consti-

tutional example of execution means of the verification means of the second embodiment;

Fig. 14 is a flow chart showing functions of the constitutional example of the execution means shown in Fig. 13;

Fig. 15 is a block diagram showing the constitution of a proving device of a third embodiment of the device for authenticating user's access rights to resources according to the present invention;

Fig. 16 is a flow chart showing functions of means constituting the proving device of the third embodiment;

Fig. 17 is a block diagram showing a constitutional example of a fourth embodiment of the device for authenticating user's access rights to resources according to the present invention;

Fig. 18 is a block diagram showing another constitutional example of the fourth embodiment;

Fig. 19 is a flow chart showing functions of means of the constitutional example shown in Fig. 17;

Fig. 20 is a block diagram showing the constitution of a fifth embodiment of the device for authenticating user's access rights to resources according to the present invention;

Fig. 21 is a flow chart showing functions of means constituting a verification device of the fifth embodiment;

Fig. 22 is a block diagram showing the constitution of a sixth embodiment of the device for authenticating user's access rights to resources according to the present invention;

Fig. 23 is a flow chart showing functions of means constituting devices of the sixth embodiment;

Fig. 24 is a block diagram showing the constitution of a seventh embodiment of the device for authenticating user's access rights to resources according to the present invention;

Fig. 25 is a flow chart showing functions of means constituting devices of the seventh embodiment; and

Fig. 26 is a block diagram showing a part of constitution of a proving device of ninth and tenth embodiments of the device for authenticating user's access rights to resources according to the present invention.

At first, an example of the fundamental constitution of the present invention is described. The user authentication system of the example can be applied to privacy protection of electronic mails or control of access to files or computer resources as well as control of execution of applications.

In Fig. 1, the user authentication system comprises a verification device 10 and a proving device 11: the proving device 11 receives an access ticket (proof support data) from an access ticket generation device 12; the verification device 10 executes a verification routine 15; the proving device 11 retains user identifying information 16 and the access ticket 13 and executes a response generation program 17.

The access ticket generation device 12 is installed in the protector side, such as an application provider. The access ticket generation device 12 generates the access ticket 13 based on unique security characteristic information of the device 14 and the user identifying information 16 and the access ticket 13 is forwarded to the user through communication or sending of a floppy-diskette or the like to be retained by the proving device 11 of the user. Then the verification device 10 sends challenging data 18 to the proving device 11. The proving device 11 generates a response 19 by utilizing the access ticket 13 and the user identifying information 16, and returns it to the verification device 10. The verification device 10 verifies the legitimacy of the response based on the challenging data, that is, the verification device 10 verifies that the response has been generated based on the challenging data and the unique security characteristic information of the device.

If the legitimacy of the response is verified, the access rights of the user is authenticated; accordingly, continuation of execution of a program, access to files, and so forth, are permitted.

With the above constitution, an example of execution control of an application program is now described.

In the above constitution, a user of an application program retains only one piece of user identifying information 16. The user identifying information is equivalent to a password in the password authentication and is unique, significant information which identifies the user. If it is possible for the user to copy and distribute the user identifying information 16, it will lead to the use of the application program by the user without legitimate access rights; therefore, the user identifying information 16 is protected by protection means 160 so that even the user who is a legitimate owner of the user identifying information 16 cannot steal it. The protection means 160 may be a hardware with a protecting effect (hereinafter referred to as tamper-resistant hardware) against theft of the inside conditions by external probes. A method of implementation of the tamper-resistant hardware will be described later.

In addition to the user identifying information 16, the response generation program 17 which executes predetermined computations is provided to the user. The program 17 performs communication with a user authentication routine (verification routine 15): on receiving two parameters, namely, the user identifying information 16 and the access ticket 13, the program 17 executes computations to arbitrary inputted values to generate the response 19 for identifying the user. The user identifying information 16 is used in the course of the computation, and it is required to protect at least a part of the program 17 by the protection means 160 since leakage of the user identifying information 16 to the outside will cause a problem by the above-described reason.

Hereinafter, memory means for storing the user identifying information and a part of the program which

are protected by the protection means 160, device for executing the part of the program (for example, consisting of a memory and a MPU) and the protection means 160 are integrally referred to as token (shown by the reference numeral 20 in Fig. 1). The token may have portability, like a smart card.

Similar to the conventional execution control technologies, the verification routine 15 is set to the application program. The verification routine 15 is same as that of the conventional technologies in that it communicates with the response generation program 17 retained by the user, and continues execution of the program if and only if a returned result (response 18) is correct. Therefore, it is necessary that the program creator knows the method of computing the combination of transferred data (challenging data 18) and correct returned data corresponding thereto (response 19).

Some examples of functions of the verification routine 15 are explained as follows:

1. Data to be transferred (challenging data 18) and expected returned data (expected value) are embedded in the verification routine 15. The verification routine 15 fetches the data to be transferred and transfers it to the user, and receives the returned data from the user. Then the verification routine 15 compares the returned data from the user with the expected value: if they are identical with each other, the verification routine 15 executes the next step of the program; if they are not identical, the verification routine 15 halts the execution of the program.

In the case where the returned data is assumed to be a result of encryption of the transferred data in accordance with a predetermined encryption algorithm, the unique security characteristic information of the device is an encryption key.

2. Data to be transferred (challenging data 18) and data generated by applying a one-way function to expected returned data (expected value) are embedded in the verification routine 15. The verification routine 15 fetches the data to be transferred and transfers it to the user, and receives the returned data from the user. Then the verification routine 15 compares data generated by applying the one-way function to the returned data from the user with the expected value: if they are identical with each other, the verification routine 15 executes the next step of the program; if they are not identical, the verification routine 15 halts the execution of the program.

In the case where the returned data is assumed to be a result of encryption of the transferred data in accordance with a predetermined encryption algorithm, the unique security characteristic information of the device is an encryption key.

3. Protection is provided by encrypting a part of code of the application program in accordance with a predetermined encryption algorithm so that execution of the program may be impossible. The verification routine 15 transfers the encrypted code to the user and receives returned data from the user, and then replace the received value with the encrypted code.

With this constitution, execution of the program may be possible if and only if the returned data is a correct decryption of the encrypted code. In this case, the unique security characteristic information is a decryption key for decrypting the encrypted code.

4. Protection is provided by encrypting a part of code of the application program in accordance with a predetermined encryption algorithm so that execution of the program may be impossible. Moreover, data generated by encrypting a decryption key paired with the encryption key used for encrypting the code is embedded as transferred data in the verification routine 15. The verification routine 15 transfers the encrypted decryption key to the user and receives returned data from the user, and then decrypts the encrypted code with the value of the received data as a decryption key.

With this constitution, the encrypted code is correctly decrypted if and only if the returned data is a decryption key which has been correctly decrypted, and accordingly execution of the program becomes possible. In this case, the unique security characteristic information of the device is a decryption key for decrypting the encrypted decryption key.

In the conventional execution control technologies, the user identifying information (authentication key of the user) is identical with the unique security characteristic information of the device. The conventional response generation routine receives the unique security characteristic information and the data transferred from the verification routine as the input, and then executes computations thereto for generating data to be returned.

By contrast, the present invention is characterized in that the user identifying information 16 and the unique security characteristic information of the device 14 are independent of each other. In this constitutional example, the response generation program 17 adds the access ticket 13 to the user identifying information 16 and the data transferred from the verification routine 15 (challenging data 18) as the input, and then executes predetermined computations to them for generating the data to be returned (response 19). The constitution has the following properties:

1. The access ticket 13 is the data calculated based on the specific user identifying information 16 and the unique security characteristic information of the device.

2. At least from the viewpoint of the computation amount, it is impossible to calculate the unique

security characteristic information from the access ticket 13 without knowing the user identifying information 16.

3. The response generation program 17 executes computations for generating correct data to be returned if and only if a correct combination of the user identifying information 16 and the access ticket 13. Note that the access ticket 13 has been calculated based on the user identifying information 16.

With the constitution described so far, the execution control can be carried out by the following steps: the user has the user identifying information 16 in advance; the program creator prepares the application program independent of the user identifying information 16 retained by the user; and the program creator generates the access ticket 13 based on the user identifying information 16 and the unique security characteristic information of the device 16 used in creating the application program and distributes the access ticket 13 to the user.

It may be possible to constitute the user identifying information 16 by two pieces of user identifying information for distinguishing the information used for preparing the access ticket 13 from the information used in a communication program by the user. In the most representative example, the user identifying information 16 is made to be a public key pair: the public key is published to be used for generating the access ticket; and the individual key is confined within the token 20 as user's individual secret information. In this case, it is possible to calculate the access ticket 13 while the user identifying information 16 is kept secret by calculating the access ticket 13 from the unique security characteristic information 14 and the public key of the public key pair.

First Embodiment

In a first embodiment, an access ticket t is defined as the relation (1).

$$t = D - e + \omega \phi (n) \quad (1)$$

In the following bulleted paragraphs, symbols used in the above relation are described.

- An integer n is an RSA modulus, hence, a product of two very large prime numbers p and q ($n = pq$).
- ϕ (n) denotes the Euler number of n, hence, a product of two integers p-1 and q-1 ($\phi(n) = (p-1)(q-1)$).
- A piece of user identifying information e is an integer allocated to each user. A piece of user identifying information is unique to a user: a different user identifying information is allocated to a different user.
- An access-ticket secret key D is a private key of an RSA public key pair. Since the modulus is assumed to be n, the relation 2 is derived from the definition.

$$\gcd (D, \phi(n)) = 1 \quad (2)$$

- In the above, gcd (x, y) denotes the greatest common divisor of two integers x and y. The existence of an integer E satisfying the relation (3), which is called an access-ticket public key, is derived from the relation (2).

$$ED \bmod \phi(n) = 1 \quad (3)$$

- ω is an integer dependent upon both n and e. It is required that a probably different value will be allocated to ω if at least one of n and e is different. In defining ω in a consistent manner, a one-way hash function h may be used.

$$\omega = h (n \mid e) \quad (4)$$

In the relation (4), n | e denotes the concatenation of the two bit-string representations of n and e. A one way hash function h is a function having the property that it is extremely difficult to calculate two distinct x and y satisfying $h(x) = h(y)$. Known examples of one-way hash functions are the MD2, MD4 and MD5 of RSA Data Securities Inc., and the standard SHS (Secure Hash Standard) of the U.S. federal government.

Among the above numbers, t, E and n can be open to public without any risk, while the rest of the numbers, namely D, e, ω, p, q and ϕ (n), are to be kept secret to everybody but those who are allowed to generate an access ticket. Fig. 3 depicts the constitution of the first embodiment. A verification device 10 comprises the followings: an access ticket public key storing means 101; a random number generation means 102; a random number storing means 103; a response storing means 105; a verification means 106; an execution means 107; and an error trapping means 108. On the other hand, a proving device 11 comprises the followings: a challenging data storing means 111; a first calculation means 112; an access ticket storing means 113; a second calculation means 114; a user identifying information storing means 115; and a response generation means 116.

By the following numbered paragraphs, the function of the means constituting the devices will be described.

1. The verification device 10 is invoked by a user. The way to invoke the device varies depending upon how the device is implemented. A few examples are now shown. First, the verification device 10 may be implemented as a part of an application program to be installed and executed on a user's PC or workstation. In this case, the user may invoke the verification device 10 by invoking the application program in ordinary ways. For example, the user may click the iconic symbol representing the application program on the computer screen with a pointing device such as a mouse, or may use a keyboard. The verification device 10 may be implemented as a program installed and executed on a

server computer that is connected to a user's PC or workstation by means of computer network. In this case, in order to invoke the verification device 10, a user first invokes a communication program installed on his/her own PC or workstation: the communication program establishes a connection to the server, and asks the server to invoke the verification device 10. When the communication program and the server follow the TCP/IP protocols, for instance, the verification device 10 is allocated to a predefined port number on the server computer. When the communication program issues a requirement for establishing a connection to the port, inetd, a demon program running on the server computer, receives the requirement. After checking which program is allocated to the specified port, it finally invokes the verification device 10, and establishes a connection between the verification device and the communication program. This way of implementation is very common in networked computer systems like Internet. The verification device 10 may be implemented as a program written on a ROM or EEPROM within a smart card reader-writer. In this case, the proving device 11 is a program installed on an IC chip of a smart card; the verification device 10 is invoked whenever a user inserts his/her smart card into the smart card reader-writer.

2. The verification device 10 sends challenging data C and a modulus n to the challenging data storing means 111 of the proving device 11. The modulus n is stored in the access-ticket public key storing means 101. On the other hand, challenging data C is generated as follows: the random number generation means 102 generates a random integer r so that r and the modulus n are relatively prime ($gcd(r, n) = 1$); the generated random integer r is stored in the random number storing means 103; finally, the random number generation means 102 sets the value of C to r. As stated later in more detail, the response which the proving device 11 is to respond to the verification device 10 is RSA-encryption of r with D as the key and n as the modulus. Since the value of C is identical to the random integer r, it varies with occurrence of communication between the verification device 10 and the proving device 11. This prevents so-called replay attack from succeeding.

3. The first calculation means 112 of the proving device 11 calculates an intermediate result R' according to the relation (5). An access ticket t to be used is stored in the access ticket storing means 113.

$$R' = C^t \bmod n \quad (5)$$

4. The second calculation means 114 of the proving device 11 calculates a differential S according to the relation (6). A user identifying information e to be used is stored in the user identifying information storing means 115.

$$S = C^e \bmod n \quad (6)$$

5. Receiving R' and S from the first calculation means 112 and the second calculation means 114, the response generation means 116 of the proving device 11 calculates a response R according to the relation (7).

$$R = R'S \bmod n \quad (7)$$

6. The proving device 11 returns the generated response R to the response storing means 105 of the verification device 10.

7. The verification means 106 of the verification device 10 first performs the calculation (8). Both the exponent E and the modulus n are stored in the access ticket public key storing means 101, and the response R is stored in the response storing means 105.

$$R^E \bmod n \quad (8)$$

Finally, the verification means 106 examines the relation (9).

$$C \bmod n = R^E \bmod n \quad (9)$$

If the relation (9) holds, the verification means invokes the execution means 107. The execution means 107 provides a user with utilities that he/she wanted to access to. Otherwise, it invokes the error trapping means 108. The error trapping means 108 may deny user access by terminating the execution.

Second Embodiment

A second embodiment to be described is the same as the first embodiment regarding the definition of an access ticket t and the function of the proving device. However, the verification device works differently. The difference in the roles between challenging data C and a response R causes the difference in the function between the two embodiments: in the first embodiment, a response R is encryption of a random challenging data C; in the second embodiment, a response R will be decryption of challenging data C which is encryption of some other meaningful data.

Fig. 5 depicts the constitution of devices of the second embodiment, and Fig. 6 depicts flow of data. A verification device 10 comprises the following means: an access ticket public key storing means 101; a random number generation means 102; a random number storing means 103; a response storing means 105; a randomizing means 121; a challenge seed storing means

122; a de-randomizing means 123; and an execution means 310. A proving device 11 comprises the following means: a challenging data storing means 111; a first calculation means 102; an access ticket storing means 113; a second calculation means 114; a user identifying information storing means 115; and a response generation means 116.

By the following numbered paragraphs, the function of the means constituting the devices will be described step by step.

1. The verification device 10 is invoked by a user.
2. The verification device 10 sends challenging data C and a modulus n to the challenging data storing means 111 of the proving device 11. The modulus n is stored in the access ticket public key storing means 101. On the other hand, challenging data C is generated by carrying out the following steps: the random number generating means 102 generates a random integer r so that r and the modulus n are relatively prime (gcd (r, n) = 1); the random integer r is stored in the random number storing means 103; the randomizing means 121 generates challenging data C according to the relation (10).

$$C = r^{E} C' \bmod n \qquad (10)$$

The integer C' is stored in the challenge seed storing means 122, and satisfies the relation (11) for some data K.

$$C' = K^{E} \bmod n \qquad (11)$$

The exponent E (access ticket public key) and the modulus n are both stored in the access ticket public key storing means 101.

The verification device 10 retains encryption C' of K instead of K itself. In fact, C' is RSA encryption of K with a public key E and a modulus n. This has an advantage in the viewpoint of security: the data K crucial for authentication procedures never leaks from the verification device 10. The randomness of r also plays an important role: if r were identical to some secret constant, the challenging data C would be encryption of the data K up to a constant coefficient, and therefore the response which the proving device 11 generates would be K up to a constant coefficient; thus, constant r would allow replay attacks since communication between the verification device 10 and the proving device 11 would be always identical. In this embodiment, by generating challenging data C so that it is dependent on a random number r (see the relation (10)), communication between the verification device 10 and the proving device 11 occurs with variation, and therefore attempts of replay attacks become hopeless.
3. The first calculation means 112 of the proving device 11 calculates an intermediate result R' according to the relation (12).

$$R' = C^{t} \bmod n \qquad (12)$$

In course of calculation, the means uses the access ticket t stored in the access ticket storing means 113.
4. The second calculation means 114 of the proving device 11 calculates a differential S according to the relation (13).

$$S = C^{e} \bmod n \qquad (13)$$

In course of calculation, the means uses the user identifying information e stored in the user identifying information storing means 115.
5. Receiving the intermediate result R' and the differential S from the first calculation means 112 and the second calculation means 114, the response generation means 116 of the proving device calculates a response R according to the relation (14).

$$R = R'S \bmod n \qquad (14)$$

6. The proving device 11 returns the generated response R to the response storing means 307 of the verification device 10.
7. The de-randomizing means 123 of the verification device 10 calculates K' according to the relation (15).

$$K' = r^{-1} R \bmod n \qquad (15)$$

In course of calculation, the means uses the random number r stored in the random number storing means 103 and the response R stored in the response storing means 105. Note that the values K' and K are identical with each other, if and only if the proving device 11 calculated the response R based on a right pair of an access ticket t and a user identifying information e.

Finally, the de-randomizing means 123 sends K' to the execution means 310, and the execution means 310 executes predefined procedures using this given K'. The execution means 310 is designed so that it works properly only when K' is identical with K; otherwise it fails to work.

The following paragraphs describes several examples of implementation of the execution means 310.

1. Fig. 7 depicts a first example. A memory means 310 a of the execution means 310 retains the data K. Receiving K' from the de-randomizing means 123, a comparison means 310b directly examines

the equality K = K'. If the equality does not hold, the execution means 310 suspends its performance immediately. Otherwise, the execution means 310 continues its performance and provides users with utilities. This example includes the disadvantage caused from the fact that the data K critical for authentication procedures appears as it is in the device: when a computer program to be installed and executed on a user's PC or workstation is implemented on the execution means 310, it is not impossible for a user to find out the value K by analyzing the code of the application program. The value K is crucial, because, if once the user knows the value of K, and further if he/she can predict random number sequences to be generated by the random number generation means 102, he/she can construct a device simulating the proving device 10 without any of an access ticket and a user identifying information e. In other words, anybody could pass the authentication check by the verification device 10 with this simulator, whether he/she is authorized or not.

2. Fig. 9 depicts a second example. In this example, a memory means 310a retains h(K), instead of K, which is a value obtained by applying a one-way hash function h to K. A significant property of one-way hash functions is that it is computationally impossible to calculate x satisfying y = h(x) given y. Receiving K' from a de-randomizing means 123, a hashing means 310c calculates h(K') which is the result of applying the one-way hash function h to K'.

Then, the comparison means 310b examines the identity of this h(K') and the value stored in the memory means 310a (= h(K)). Compared with the first example, this example is safer since there is no effective means to find out the critical data K: even though a user succeeded in analyzing the code of the program constituting the execution means 310, he/she couldn't find out any more than the value of h(K); due to the property of one-way hash functions, it is computationally impossible to calculate K given h(K). However, when the execution means 310 is implemented as a computer program, the comparison means 310b may be represented as an if-clause. If the verification device is further assumed to be executed on a user's PC or workstation, a user may have a chance to modify the code so that the if-clause shall be always skipped.

Therefore, the implementation of the this example is not safe enough, in particular, if the execution means 310 is implemented as a computer program to be executed on a user's PC or workstation.

3. Fig. 11 depicts a third example. This time, protection is applied such that execution of the program of the execution means 310 becomes impossible by encrypting a portion or the whole of the code of the program. The encrypted code is stored in the challenge seed storing means 122 as a seed C' for challenging data C. More precisely, the crucial data K is program code to be encrypted, and C' is RSA encryption of the code K with a public key E and a modulus n (C = KE mod n). Both E and n are the values stored in the access ticket public key storing means 101. The execution means 310 includes a code storing means 310d, a code loading means 310e and a code execution means 310f. The code loading means 310e feeds K', which the code storing means 310d received from the de-randomizing means 123, to the code execution means 310f. Only when K' is identical with K, the code fed to the code execution means 310f is meaningful as a part of the program of the execution means 310. In the following, a more detailed description of the composition is provided. Consider the case where the execution means 310 is implemented as a computer program executed on a user's PC or workstation. The code storing means 310d is a specified region within a memory of a user's PC.

The code execution means 310f comprises the CPU and OS of the PC. The CPU and OS, cooperating with each other, fetch instructions form a certain predefined region within the memory space (called program region), and executes those instructions one by one. Generally speaking, a meaningful chunk of instructions is called a program, and a program is located within the program region. The entity of the code loading means 310e is a part of the program constituting the execution means 310, and it is to be executed at first when the execution means 310 is invoked. When invoked, the code loading means 310e orders the code execution means 310f to copy the content stored in the code storing means 310d onto a specified area within the program region, and then orders the code execution means 310f to execute the copied sequence of instructions by issuing a JMP command, for example.

Thus, since a part or the whole of the code of the program of the execution means 310 is encrypted, and further since it is decrypted temporarily only when the verification device 10 and the proving device 11 cooperate with each other properly, the execution means 310 is much safer than in the cases of the preceding two examples: even though a user succeeded in analyzing the program, he/she couldn't obtain the missing code K at all; modifying the code of the program without the knowledge about K is definitely no use.

4. Fig. 13 depicts a fourth example. This example is substantially the same as the third example except that K is the encryption key used in encrypting code of the program constituting the execution means 310, while K is the code itself in the previous example. Since the code to be encrypted may be of large size, according to the composition of the third example, the size of K (namely, that of C' and C) may be large enough to make the performance of the verification device 10 and the proving device 11

worse. In contrast, according to the composition of the fourth example, the size of K (namely, that of C') remains unchanged irrespective of the size of the program code to be encrypted: the size of K is determined by the cipher algorithm to be used; if DES (Data Encryption Standard) is used, K is always 64 (56) bits long even when the size of the code to be encrypted is measured by Mbyte.

The execution means 310 comprises an encrypted code storing means 310g, a decryption means 310h, a code loading means 310l, and code execution means 310f. Receiving the data K' from the de-randomizing means 123, the decryption means 310h decrypts the content stored in the encrypted code storing means 310g. In the process of decryption, K' is used as a decryption key. The code loading means 310l loads the output of the decryption means 310h, which is decrypted code if K' is identical with K, onto a specified area within the program region, and then orders the execution means 310f to execute the loaded code.

Third Embodiment

In a third embodiment, the definition of an access ticket is given as the relation (16).

$$t = D + F(n, e) \quad (16)$$

The following bulleted paragraphs illustrate the symbols appearing in the relation (16).

- An integer n is an RSA modulus, hence, a product of two very large prime numbers p and q ($n = pq$).
- $\phi(n)$ denotes the Euler number of n, hence, a product of two integers p-1 and q-1 ($\phi(n) = (p-1)(q-1)$).
- A user identifying information e is an integer allocated to each user. The user identifying information e is unique to each user:
- A different user identifying information is allocated to a different user.
- An access-ticket secret key D is the private key of an RSA public key pair. Since the assumed modulus is n, D satisfies the relation (17).

$$\gcd(D, \phi(n)) = 1 \quad (17)$$

- In the above, gcd(x, y) denotes the greatest common divisor of two integers x and y. The existence of an integer E satisfying the relation (18), which is called an access-ticket public key, is derived form the relation 17.

$$ED \bmod \phi(n) = 1 \quad (18)$$

- A two variable function F(x, y) is an arbitrary collision-free function. Practically, a collision-free function may be constructed using a one-way hash function h as the relation (19).

$$F(x, y) = h(x \mid y) \quad (19)$$

Figs. 15 and 16 are for depicting this embodiment: Fig. 15 depicts the constitution of the devices of this embodiment; Fig. 16 depicts flow of data.

In Fig. 15, a proving device 11 comprises a challenging data storing means 111, a first calculation means 112, an access ticket storing means 113, a second calculation means 114, a user identifying information storing means 115, a response generation means 116, and an exponent generation means 130. A verification device 10 in this embodiment may be identical with that in any of the first embodiment (shown in Fig. 3) or the second embodiment (shown in Fig. 5).

By the following numbered paragraphs, the function of the means constituting the devices will be described step by step.

1. The verification device 10 is invoked by a user.
2. The verification device 10 sends challenging data C and a modulus n to the challenging data storing means 111 of the proving device 11. The modulus n is stored in the access ticket public key storing means 101, and the challenging data C is generated in one of the manners defined in the first embodiment or the second embodiment: C is identical with either $r^E \bmod n$ or $r^E C' \bmod n$.
3. The first calculation means 112 of the proving device 11 calculates an intermediate result R' according to the relation (20). An access ticket t to be used is stored in the access ticket storing means 113.

$$R' = C^t \bmod n \quad (20)$$

4. The exponent generation means 130 calculates F(n, e) by applying the collision-free function F to the modulus n, stored in the challenging data storing means 111, and the user identifying information e, stored in the user identifying information storing means 115.

$$F(n, e) \quad (21)$$

5. Receiving the result from the exponent generation means 130, the second calculation means 114 of the proving device 11 calculates a differential S according to the relation (22).

$$S = C^{F(n, e)} \bmod n \quad (22)$$

6. Receiving R' and S from the first calculation means 112 and the second calculation means 114, the response generation means 116 of the proving device calculates a response R according to the relation (23).

$$R = R'S^{-1} \bmod n \quad (23)$$

In the relation (23), S^{-1} denotes the reciprocal of S under the modulus n. Hence, S and S^{-1} satisfy the relation (24).

$$SS^{-1} \bmod n = 1 \quad (24)$$

7. The proving device 11 returns the generated response R to the response storing means 105 of the verification device 10.
8. The verification device 10 examines the response received from the proving device 11.

Fourth Embodiment

In a fourth embodiment, a proving device 11 comprises a computer program executed on a user's PC or workstation, a smart card or PC card (PCMCIA card) attachable to the user's PC or workstation, and a program executed on this smart card or PC card.

As is obvious from the explanation of the former three embodiments, a user identifying information e, stored in a user identifying information storing means 115, must be kept secret to others. Furthermore, observing process of execution of a second calculation means 114, which needs e as an input to itself, may lead to leak of e. The same situation applies to an exponent generation means 130. Consequently, in practical use, the user identifying information storing means 115, the second calculation means 114 and the exponent generation means 130 should be protected by some means against attempts to pry out some crucial secret out of them.

One solution is confining the crucial part of the proving device 11 within hardware equipped with function to prevent its inside from being observed or tampered with by unauthorized means. Generally, such hardware is called tamper-resistant hardware.

In creating the tamper-resistant hardware, it is possible to use the technology disclosed in Patent Number 1,863,953, Patent Number 1,860,463 or Japanese Laid-Open Patent Publication 3-100753, for example. In Patent Number 1,863,953, an enclosure composed of a plurality of cards having multi-layered conductive patterns is provided surrounding an information memory medium. Memory information is destroyed when the conductive pattern which is detected differs from an expected pattern.

In Patent Number 1,860,463, a detection circuit composed of an integration circuit or the like is provided surrounding an information memory medium in addition to a conductive winding being formed, and through this, when there is infiltration to the electronic circuit region, fluctuations in electromagnetic energy are detected and memory information is destroyed.

In Japanese Laid-Open Patent Publication 3-100753, an optical detector is provided within hardware, and the optical detector detects external light which enters when a force is applied which destroys the hardware or punctures the hardware, and a memory destruction device resets memory information.

Further, choosing tamper-resistant hardware with portability such as a smart card or PC card may provide users with additional merits. Among information dealt with by a proving device 11, only an access ticket and a user identifying information are unique to an individual user. Hence, for example, it may be useful to confine a user identifying information storing means 115, access ticket storing means 113, a second calculation means 114 and exponent generation means 130 within a smart card or PC card, and implement the rest of the proving device 10 as a program to be executed on an arbitrary PC or workstation: a user can use an arbitrary PC or workstation, assuming that the program is installed on it, as his/her proving device only by inserting his/her own smart card or PC card into the computer.

Fig. 17 depicts constitution of a proving device 11 of the first and second embodiments when a user identifying information storing means 115 and a second calculation means 114 are confined within a smart card.

Fig. 18 depicts constitution of a proving device 11 of the third embodiment when a exponent generation means 130 in addition to a user identifying information storing means 114 and a second calculation means 114 is confined within a smart card.

For both Figs. 17 and 18, a card-side I/F means 141 within a smart card is an interface to a host computer for communication between a host computer and the smart card. More practically, the card-side I/F means 141 comprises buffer memory and a communication program.

A host-side I/F means 140, which is a part of a host computer, is the counter part of the card-side I/F means 141. Both I/F means, cooperating with each other, transfer messages from the host computer to the smart card, and vice versa.

The following numbered paragraphs describe the function of the means constituting the devices.

1. The verification device 10 is invoked by a user.
2. The verification device 10 sends challenging data C and a modulus n stored in the access ticket public key storing means 101 to the challenging data storing means 111 of the proving device 11.
3. The host-side I/F means 140 of the proving device 10 sends the challenging data C and the modulus n to the card-side I/F means 141 within the smart card.
4. The access ticket searching means 142 retrieves an access ticket t corresponding to the modulus n that is stored in the challenging data storing means 111. As shown before, in any of the former three embodiments, the definition of an access ticket t involves a modulus n ($t = D - e + \omega\,\phi(n)$ or $t = D + F(n, e)$). In the access ticket storing means 113, zero or more access ticket are stored, and each access ticket is indexed with the modulus that was used in generating the access ticket.

5. The first calculation means 112 of the proving device 11 calculates an intermediate result R' according to the relation (25).
An access ticket t is stored in the access ticket storing means 113.

$$R' = C^t \bmod n \quad (25)$$

6. The host-side I/F means 140 issues a requirement for a differential S to the card-side I/F means 141. A response which the host-side I/F means 140 receives is a differential S of one of the following forms: if the access ticket t and the means within the smart card were implemented in the manner of the first and second embodiments, the differential S satisfies the relation (26); if the access ticket t and the means within the smart card were implemented in the manner of the third embodiment, the differential S satisfies the relation (27).

$$S = C^e \bmod n \quad (26)$$

$$S = C^{F(n, e)} \bmod n \quad (27)$$

7. The response generation means 116 of the proving device 11 calculates a response R according to either the relation (28) or (29): if the access ticket t and the means within the smart card were implemented in the manner of the first and second embodiments, the relation (28) shall be applied; if the access ticket t and the means within the smart card were implemented in the manner of the third embodiment, the relation (29) shall be applied.

$$R = R'S \bmod n \quad (28)$$

$$R = R'S^{-1} \bmod n \quad (29)$$

8. The proving device 11 returns the generated response R to the response storing means 307 of the verification device 10.

In this embodiment, it is possible to calculate the intermediate result R' and the differential S concurrently, because the former is calculated within the host computer and the latter is within the smart card. Obviously, this concurrent calculation reduces the total time which the proving device 11 needs for calculating a response to a received challenging data.

Further, in this embodiment, the access ticket storing means 113 may retain more than one access tickets, and the access ticket searching means 142 retrieves an appropriate access ticket using a modulus issued by the verification device 10 as a key for retrieval. Basically, different verification device, which may be embedded within a different application program or server program, should assume a different modulus. Therefore, a user who want to access to more than one application programs or server programs is obliged to have a number of access tickets.

The stated function of the access ticket searching means 142 would release a user from paraphernalia of selecting a correct access ticket by himself.

Fifth Embodiment

In a fifth embodiment, the Pohlig-Hellman asymmetric key cryptography is used instead of the RSA public key cryptography.

In this embodiment, the definition of an access ticket t is given as the relation (30).

$$t = D + F(p, e) \quad (30)$$

The following bulleted paragraphs illustrate the symbols appearing in the relation (30).

- An integer p is a very large prime number.
- A user identifying information e is an integer allocated to each user. The user identifying information e is unique to an individual user: a different user identifying information is allocated to a different user.
- An access ticket secret key D is one component of a Pohlig-Hellman asymmetric key pair. Since the assumed modulus is p, D satisfies the relation (31).

$$\gcd(D, p-1) = 1 \quad (31)$$

In the above, gcd(x, y) denotes the greatest common divisor of two integers x and y. The existence of an integer E satisfying the relation (32), which is called an access-ticket public key, is derived from the relation (31).

$$ED \bmod p-1 = 1 \quad (32)$$

- A two variable function F(x, y) is an arbitrary collision-free function. Practically, a collision-free function may be constructed using a one-way hash function h as the relation (33).

$$F(x, y) = h(x \mid y) \quad (33)$$

Figs. 20 and 21 are for depicting this embodiment: Fig. 20 depicts the constitution of the devices of this embodiment; Fig. 21 depicts flow of data. In Fig. 20, a proving device 41 comprises the following means: a challenging data storing means 411; a first calculation means 412; an access ticket storing means 413; a second calculation means 414; a user identifying information storing means 415; a response generation means 416; and an exponent generation means 430. On the other hand, a verification device 40 comprises the following means: a key storing means 401; a random number generation means 402; a random number storing means 403; a response storing means 405; a randomizing means 421; a challenging seed storing means

422; a de-randomizing means 423; and an execution means 310.

By the following numbered paragraphs, the function of the means constituting the devices will be described step by step.

1. The verification device 40 is invoked by a user.
2. The verification device 40 sends challenging data C and a modulus p to the challenging data storing means 411 of the proving device 41. The modulus p is stored in the key storing means 401. In this embodiment, the challenging data C is assumed to be generated in a manner similar to that in the second embodiment. However, it is easy to construct another embodiment such that challenging data C is generated in a manner similar to that in the first embodiment. The challenging data C in this embodiment is generated by carrying out the following steps: the random number generating means 402 generates a random integer r so that r and the modulus p are relatively prime ($gcd(r, p) = 1$); the random integer r is stored in the random number storing means 403; and the randomizing means 121 generates challenging data C according to the relation (34).

$$C = r^{E}C' \bmod p \quad (34)$$

The integer C' is stored in the challenge seed storing means 422, and satisfies the relation (35) for some data K.

$$C' = K^{E} \bmod p \quad (35)$$

The exponent E (access ticket public key) and the modulus p are both stored in the key storing means 401.
3. The first calculation means 412 of the proving device 41 calculates an intermediate result R' according to the relation 36.
An access ticket t to be used is stored in the access ticket storing means 113.

$$R' = C^{t} \bmod p \quad (36)$$

4. The exponent generation means 430 calculates F(p, e) by applying the collision-free function F to the modulus p, stored in the challenging data storing means 111, and the user identifying information e, stored in the user identifying information storing means 415.

$$F(p, e) \quad (37)$$

5. Receiving the result from the exponent generation means 430, the second calculation means 414 of the proving device 41 calculates a differential S according to the relation (38).

$$S = C^{F(p, e)} \bmod p \quad (38)$$

6. Receiving R' and S from the first calculation means 412 and the second calculation means 414, the response generation means 416 of the proving device 41 calculates a response R according to the relation (39).

$$R = R'S^{-1} \bmod p \quad (39)$$

In the relation (39), S^{-1} denotes the reciprocal of S under the modulus p. Hence, S and S^{-1} satisfy the relation (40).

$$SS^{-1} \bmod p = 1 \quad (40)$$

7. The proving device 41 returns the generated response R to the response storing means 405 of the verification device 40.
8. The de-randomizing means 423 of the verification device 40 calculates K' according to the relation (41).

$$K' = r^{-1}R \bmod p \quad (41)$$

In course of calculation, the means uses the random number r stored in the random number storing means 403 and the response R stored in the response storing means 405.

Sixth Embodiment

A sixth embodiment is substantially similar to the third embodiment except that the ElGamal public key cryptography is used this time instead of the RSA public key cryptgraphy. In this embodiment, the definition of an access ticket t is given as the relation (42).

$$t = X + F(p, e) \quad (42)$$

The following bulleted paragraphs illustrate the symbols appearing in the relation (42).

- An integer p is a very large prime number.
- A user identifying information e is an integer allocated to each user. The user identifying information is unique to an individual user: a different user identifying information is allocated to a different user.
- Let (X, Y) be an arbitrary ElGamal asymmetric key pair assuming p is the modulus. Therefore the relation (43) is satisfied.

$$Y = G^{X} \bmod p \quad (43)$$

In the relation (43), G denotes an integer representing a generator of the multiplicative group of the finite field of order p.

- Equivalently, G satisfies the relations (44) and (45).

$$G > 0 \quad (44)$$

$$\min \{ x>0 \mid G^X = 1 \bmod p\} = p - 1 \quad (45)$$

- X is called an access ticket secret key, while Y is called an access ticket public key.
- A two variable function F(x, y) is an arbitrary collision-free function. Practically, a collision-free function may be constructed using a one-way hash function h as the relation (46).

$$F(x, y) = h(x \mid y) \quad (46)$$

Figs. 22 and 23 are for depicting this embodiment: Fig. 22 depicts the constitution of the devices of this embodiment; Fig. 23 depicts flow of data.

In Fig. 22, a proving device 51 comprises the following means: a challenging data storing means 511; a first calculation means 512; an access ticket storing means 513; a second calculation means 514; a user identifying information storing means 515; a response generation means 516; and an exponent generation means 530. On the other hand, a verification device 50 comprises the following means: an access ticket public key storing means 501; a random number generation means 502; a random number storing means 503; a response storing means 505; a randomizing means 521; a challenge seed storing means 522; a de-randomizing means 523; and an execution means 310.

By the following numbered paragraphs, the function of the means constituting the devices will be described step by step.

1. The verification device 50 is invoked by a user.
2. The verification device 50 sends a pair (u, C) of challenging data and a modulus p to the challenging data storing means 511 of the proving device 51. The modulus p is stored in the access ticket public key storing means 501. On the other hand, the challenging data u and C is generated as follows. The first component u is stored in the challenge seed storing means 522, and satisfies the relation (47) for some secret random number z.

$$u = G^z \bmod p \quad (47)$$

In the challenge seed storing means 522, one more seed C' is stored. C' satisfies the relation (48). for some crucial data K. (48) $C' = Y^2K \bmod p$

Using this C' as a seed, the other component C is generated as follows. The random number generating means 502 generates a random integer r so that r and the modulus p are relatively prime ($\gcd(r, p) = 1$); the random integer r is stored in the random number storing means 503; the randomizing means 521 generates challenging data C according to the relation (49).

$$C = rC' \bmod p \quad (49)$$

3. The first calculation means 512 of the proving device 51 calculates an intermediate result S according to the relation (50).
An access ticket t to be used is stored in the access ticket storing means 513.

$$S = u^t \bmod p \quad (50)$$

4. The exponent generation means 530 calculates F(p, e) by applying the collision-free function F to the modulus p, stored in the challenging data storing means 511, and the user identifying information e, stored in the user identifying information storing means 515.

$$F(p, e) \quad (51)$$

5. Receiving the result from the exponent generation means 530, the second calculation means 514 of the proving device 51 calculates a differential S' according to the relation (52).

$$S' = u^{F(p, e)} \bmod p \quad (52)$$

6. Receiving S and S' from the first calculation means 512 and the second calculation means 514, the response generation means 516 of the proving device 51 calculates a response R according to the relation (53).

$$R = S^{-1}S'C \bmod p \quad (53)$$

In the relation (53), S^{-1} denotes the reciprocal of S over the modulus p. Hence, S and S^{-1} satisfy the relation (54).

$$SS^{-1} \bmod p = 1 \quad (54)$$

7. The proving device 51 returns the generated response R to the response storing means 505 of the verification device 50.
8. The de-randomizing means 523 of the verification device 50 calculates K' according to the relation (55).

$$K' = r^{-1}R \bmod p \quad (55)$$

In course of calculation, the means uses the random number r stored in the random number storing means 503 and the response R stored in the response storing means 505.

The straightforward implementation of the above

constitution would involve the following problem: use of a common pair of seeds for challenging data (u, C') for more than one occurrences of authentication allows an attacker to construct a device which emulates the proving device 11 without the user identifying information or the access ticket. To construct such an emulator, $H = RC^{-1} \bmod p$ is recorded first where C is the challenging data at the first occurrence of authentication and R is the response to C calculated by the proving device 11. The emulator retains this H instead of the user identifying information e and the access ticket t, and on arbitrary input (u, C) issued by the verification device 10, returns to a response R calculated according to the relation $R = HC \bmod p$. Thus, the verification device 10 should have pairs of seeds (u^3, C') as many as necessary, and should use distinct pair for distinct occurrence of authentication (Note that k for $u = G^z \bmod p$ is a random number).

Seventh Embodiment

A seventh embodiment exploits the ElGamal signature rather than the RSA public key cryptography in the first three embodiments or the ElGamal public key cryptography in the sixth embodiment.

In this embodiment, the definition of an access ticket t is given as the relation (56).

$$t = X + F(p, e) \tag{56}$$

The following bulleted paragraphs illustrate the symbols appearing in the relation (56).

- An integer p is a very large prime number.
- A user identifying information e is an integer allocated to each user. The user identifying information e is unique to an individual user: a different user identifying information is allocated to a different user.
- Let (X, Y) be an arbitrary ElGamal asymmetric key pair assuming p is the modulus. Therefore the relation (57) is satisfied.

$$Y = G^X \bmod p \tag{57}$$

In the relation (57), G denotes an integer representing a generator of the multiplicative group of the finite field of order p.

Equivalently, an integer G satisfies the relations (58) and (59).

$$G > 0 \tag{58}$$

$$\min \{ x>0 \mid G^X = 1 \bmod p \} = p - 1 \tag{59}$$

X is called an access ticket secret key, while Y is called an access ticket public key.

- A two variable function F(x, y) is an arbitrary collision-free function. Practically, a collision-free function may be constructed using a one-way hash function h as the relation (60) shows.

$$F(x, y) = h(x \mid y) \tag{60}$$

Figs. 24 and 25 are for depicting this embodiment: Fig. 24 depicts the constitution of the devices of this embodiment; Fig. 25 depicts flow of data.

In Fig. 24, a proving device 61 comprises the following means: a challenging data storing means 611; a random number generation means 612; a first calculation means 613; a second calculation means 614; an access ticket storing means 615; and a user identifying information storing means 616. On the other hand, verification device 60 comprises the following means: an access ticket public key storing means 601; a random number generation means 602; a random number storing means 603; a response storing means 605; a verification means 606; a execution means 607; and an error trapping means 608.

By the following numbered paragraphs, the function of the means constituting the devices will be described step by step.

1. The verification device 60 is invoked by a user.
2. The verification device 60 sends challenging data C, a modulus p and a generator G to the challenging data storing means 611 of the proving device 61. The modulus p and the generator G are stored in the access ticket public key storing means 601. On the other hand, the challenging data u and C are generated as follows: the random number generation means 602 generates a random integer r so that r and the modulus n are relatively prime ($\gcd(r, n) = 1$); the generated random integer r is stored in the random number storing means 603; finally, the random number generation means 602 sets the value of C to r. As stated later in more detail, the response which the proving device 61 is to respond to the verification device 60 is ElGamal-signature of r with X as the signature key and p as the modulus.
3. The random number generation means 612 of the proving device 61 generates a random integer k so that k and p are relatively prime ($\gcd(k, p) = 1$). Receiving the random integer k from the random number generation means 612 and the modulus p and the generator G from the challenging data storing means 611, the first calculation means 613 calculates a first component R of a response according to the relation (61):

$$R = G^k \bmod p \tag{61}$$

Concurrently, the second calculation means 614 calculates a second component S of a response according to the relation (62).

$$S = (C - R(t - F(p, e)))k^{-1} \bmod p - 1 \quad (62)$$

The access ticket t is stored in the access ticket storing means 615, and the modulus p and the challenging data C are stored in the challenging data storing means 611.

4. The proving device 61 returns the generated response R to the response storing means 605 of the verification device 60.

5. The verification means 606 of the verification device 60 examines the relation (63).

$$G^r = Y^R R^S \bmod p \quad (63)$$

The random integer r is stored in the random number storing means 603; the response pair (R, S) is stored in the response storing means 605; the modulus p, the access ticket public key Y and the generator G are all stored in the access ticket public key storing means 601.

Eighth Embodiment

An eighth embodiment provides an example of specification for ways how to generate access tickets safely.

In any case of the previous embodiments, access tickets are calculated as output of a predefined function on input of specific secret information, namely user identifying information and access ticket secret keys. Since leak of that secret information threatens the safety of the entire scheme of authentication, a safe device may be necessary in generating access tickets.

Such a device is required to provide the function which absolutely prevents leakage of the secret information contained within it or results of calculations carried out within it.

One of the simplest ways to constitute such a safe device is to implement services of generating and issuing access ticket to users on an isolated computer kept safe from any attempts at illegal accesses by users: in order to protect that server computer against physical accesses by users, the computer should be placed in a room entry into which is severely controlled; further, if the server computer is networked with users' PCs and access tickets are issued to users on network, the threat of attacks via network should be taken into account; in protecting the server computer from those network attacks, the firewall technology (for details see "Building Internet Firewalls" by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, Inc.) may be useful..

As shown in the previous embodiments, an access ticket is generated so that only the user to whom the ticket is issued can use it. Speaking more accurately, a user may succeed in authentication procedure between a verification device and a proving device if and only if he is able to feed to the proving device both an access ticket and user identifying information based on which the access ticket has been generated.

Moreover, access tickets stated in the previous embodiments satisfy a stricter standard of safety: there is no way to forge an access ticket or to construct a device which emulates the proving device even though an attacker is assumed to be able to collect an arbitrary number of access tickets issued by legitimate access ticket issuers.

The fact that access ticket satisfies the above standard implies that access tickets are safe enough to be conveyed to users by relatively insecure means like electronic mails on Internet.

Ninth Embodiment

A ninth embodiment uses a composition method for an access ticket and user identifying information differing from those of the previous embodiments: this method is different from those of the previous embodiments in that the public information associated with user identifying information is used instead of the user identifying information itself in generating an access ticket.

Therefore, according to the method stated below, a safe access ticket issuing server stated in the eighth embodiment is not necessary: a user is allowed to generate an access ticket with a program executed on his own PC or workstation. That program doesn't contain any secret information or any secret algorithm.

The identifying information of a user U is the private key d_U of an RSA public key pair. By (e_U, n_U), the public key corresponding to the private key d_U is denoted. Hence, $n_U = p_U q_U$ for two distinct large prime numbers p_U and q_U, and d_U and e_U are integers determined so as to satisfy the relations (64).

$$1 \leqq d_U < (p_U - 1)(q_U - 1) \quad (64)$$

$$1 \leqq e_U < (p_U - 1)(q_U - 1)$$

$$e_U d_U = 1 \bmod (p_U - 1)(q_U - 1)$$

Hereafter, the condition that n_U is at least as large as a constant N common to all users is further assumed.

An access ticket for a user U is composed as follows: the public key (E, n) of an RSA public key pair is taken to be the public key of the access ticket to be generated; the private key D which is paired with this public key (E, n) is taken to be the secret key of the access ticket; when the prime factorization of n is $n = pq$, the relations 65 is established; finally, the access ticket t_U is defined by the relation (66).

$$1 \leqq D < N \quad (65)$$

$$DE = 1 \bmod (p - 1)(q - 1)$$

$$t_U = D^{e_U} \bmod n_U \quad (66)$$

In the above composition, the unique security char-

acteristic information for authentication process is the private key D. Same as the cases in the previous embodiments, a user succeeds in authentication procedures if and only if he is able to prove that he has means to calculate a right response to challenging data issued to him by a verification device: the calculated response is right only when it is calculated based on the unique security characteristic information D.

The composition method presented in this embodiment is characterized by the property that an access ticket is encryption of the unique security characteristic information D and the user identifying information is the unique decryption key to obtain D from the access ticket. In addition, since the user identifying information is the private key of an RSA key pair, anybody who is allowed to know the public key paired with the private key can generate an access ticket for the user at will.

Hereafter, the device composition and operation of the proving device 71 are described with reference to Fig. 26.

1. A verification device 10 sends challenging data C to a challenging data storing means 711 of a proving device 71.
2. A decryption key generation means 712 of the proving device 71 acquires user identifying information d_U which is stored in a user identifying information storing means 715 and an access ticket t_U which is stored in an access ticket storing means 713, and then calculates D' according to the relation (67).

$$D' = t_U^{dU} \bmod n_U \quad (67)$$

3. On input of D' calculated by the decryption key generation means 712 and the challenging data C stored in the challenging data storing means 711, a response generation means 714 of the proving device 71 calculates a response R according to the relation (68). The calculated response R is returned to the verification device 10.

$$R = C^{D'} \bmod n \quad (68)$$

4. The verification device 10 verifies the legitimacy of the response R.

The access ticket secret key D in the definition of the access ticket $t_U = D^e{}_U \bmod n_U$ must be kept secret to the user U. Therefore, the user identifying information storing means 713, the decryption key generation means 712 and the response generation means 714 are to be incorporated in a defense means 760 which is a tamper-resistant hardware.

The same as the cases of the previous embodiments, the verification device authenticates access rights of the user if and only if he has the right pair of the ticket t_U and the user identifying information e.

Tenth Embodiment

A tenth embodiment is substantially the same as the ninth embodiment, except that a response R is calculated using a symmetric key cipher instead of using the RSA public key cryptography as in the ninth embodiment and an access ticket is RSA-encryption of the decryption key (same as the encryption key) D of the symmetric key cipher. As the encryption key to generate the access ticket, the public key (e_U, n_U) and the RSA algorithm is used.

When the encryption function of the symmetric key encryption is expressed as Encrypt (key, plain message: the output of this function being the cipher message of the plain message which is the second argument of the function) and the decryption function is expressed as Decrypt (key, cipher message: the output being the plain message corresponding to the cipher message which is the second argument of the function), the challenging data C is defined by relation (69).

$$C = \text{Encrypt}(D, K) \quad (69)$$

Furthermore, the access ticket tU is defined by the relation (70).

$$t_U = D^{eU} \bmod n_U \quad (70)$$

Hereafter, the operation of the proving device 11 is described with reference to Fig. 26.

1. A verification device 10 sends challenging data C to a challenging data storing means 711.
2. A decryption key generation means 712 of the proving device 11 acquires user identifying information d_U which is stored in a user identifying information storing means 715 and an access ticket t_U which is stored in an access ticket storing means 713, and then calculates D' according to the relation (71).

$$D' = t_U^{dU} \bmod n_U \quad (71)$$

3. On input of D' calculated by the decryption key generation means 712 and the challenging data C stored in the challenging data storing means 711, a response generation means 714 of the proving device 11 calculates a response R according to the relation (72). The calculated response R is sent back to the verification device 10.

$$R = \text{Decrypt}(D' C) \quad (72)$$

4. The verification device 10 verifies the legitimacy of the response R.

The foregoing description of preferred embodiments of this invention has been presented for purposes of illustration and description. It is not intended to

be exhaustive or to limit the invention to the precise form disclosed, and modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. The embodiments were chosen and described in order to explain the principles of the invention and its practical application to enable one skilled in the art to utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto, and their equivalents.

Claims

1. A device for authenticating user's access rights to resources comprising:

   first memory means 111 for storing challenging data 18;
   second memory means 115 for storing unique identifying information of the user 16;
   third memory means 113 for storing proof support information 13 which is a result of executing predetermined computations to the user unique identifying information 16 and unique security characteristic information of the device 14;
   response generation means 116 for generating a response 19 from the challenging data 18 stored in the first memory means 111, the unique identifying information of the user 16 stored in the second memory means 115, and the proof support information 13 stored in the third memory means 113; and
   verification means 106 for verifying the legitimacy of the response 19 by verifying that the response 19, the challenging data 18 and the unique security characteristic information of the device 14 satisfy a specific predefined relation.

2. The device for authenticating user's access rights to resources of claim 1 further comprising:

   protect means 160 for preventing any data inside from being observed or being tampered with from the outside, at least confining the second memory means 115 and the response generation means 116.

3. The device for authenticating user's access rights to resources of claim 1, wherein

   at least the second memory means 115 and the response generation means 116 are implemented within a small portable device such as a smart card.

4. The device for authenticating user's access rights to resources of any of claims 1 through 3, wherein

   the response generation means 116 comprises:
   first calculation means 712 for replaying the unique security characteristic information of the device 14 by executing predetermined calculations to the unique identifying information of the user 16 stored in the second memory means 115 and the proof support information 13 stored in the third memory means 113; and
   second calculation means 714 for generating a response by executing predetermined calculations to the challenging data 18 stored in the first memory means 111 and the unique security characteristic information of the device 14 replayed by the first calculation means 712.

5. The device for authenticating user's access rights to resources of any of claims 1 through 3, wherein

   the response generation means 116 comprises:
   third calculation means 112 for generating first intermediate information by executing predetermined calculations to the challenging data stored in the first memory means and the proof support information stored in the third memory means;
   fourth calculation means 114 for generating second intermediate information by executing predetermined calculations to the challenging data 18 stored in the first memory means 111 and the user unique identifying information 16 stored in the second memory means 115; and
   fifth calculation means 116 for generating a response by executing predetermined calculations to the first intermediate information generated by the third calculation means 112 and the second intermediate information generated by the fourth calculation means 114.

6. The device for authenticating user's access rights to resources of claim 5, further comprising:

   protect means 160 for preventing any data inside from being observed or being tampered with from the outside, at least confining the second memory means 115 and the fourth calculation means 114.

7. The device for authenticating user's access rights to resources of claim 5, wherein

   at least the second memory means 115 and the fourth calculation means 114 are implemented within a portable device such as a smart card.

8. The device for authenticating user's access rights to resources of any of claims 1 through 7, wherein

the unique security characteristic information of the device 14 is a decryption key of a cipher function,
the challenging data 18 is encryption of information using the cipher function with the encryption key corresponding to the decryption key, and
the verification means 106 verifies the legitimacy of the response by verifying that the response 19 generated by the response generation means 116 is identical with decryption of the challenging data with the decryption key.

9. The device for authenticating user's access rights to resources of any of claims 1 through 7, wherein

the unique security characteristic information of the device 14 is an encryption key of a cipher function, and
the verification means 106 verifies the legitimacy of the response by verifying that the response 19 generated by the response generation means 116 is identical with encryption of the challenging data with the encryption key.

10. The device for authenticating user's access rights to resources of any of claims 1 through 7, wherein

the characteristic information of the device 14 is the signature key of a digital signature function, and
the verification means 106 verifies the legitimacy of the response by verifying that the response 19 generated by the response generation means 116 is identical with the digital signature for the challenging data, which is calculated with the signature key.

11. The device for authenticating user's access rights to resources of claim 8 or 9, wherein

the cipher function is of the asymmetric key cryptography, and
the unique security characteristic information of the device 14 is one component of the key pair of the cipher function.

12. The device for authenticating user's access rights to resources of claim 11, wherein

the cipher function is of the public key cryptography, and
the unique security characteristic information of the device 14 is the private key of the public key pair of the cipher function.

13. The device for authenticating user's access rights to resources of claim 8 or 9, wherein

the cipher function is of the symmetric key cryptography, and
the unique security characteristic information of the device 14 is the common key of the cipher function.

14. The device for authenticating user's access rights to resources of any of claims 1 through 13, further comprising:

a proving device 11 having the first memory means 111, the second memory means 115, the third memory means 113 and the response generation means 116; and
a verification device 10 having fourth memory means for storing the challenging data 18, fifth memory means 105 for storing the response 19 and the verification means 106, wherein
the verification device 10 transfers the challenging data 18 stored in the fourth memory means to the first memory means 111 of the proving device 11, the proving device 11 transfers the response 18 generated by the response generation means 116 to the fifth memory means 105 of the verification device 10, and the verification means 106 of the verification device 10 verifies the legitimacy of the response stored in the fifth memory means 105.

15. The device for authenticating user's access rights to resources of claim 14, wherein

the unique security characteristic information of the device 14 is an encryption key of a cipher function,
the verification device 10 comprises random number generation means 102 for generating a random number and for storing it in the fourth memory means, and
the verification means 106 verifies the legitimacy of the response by verifying that the response stored in the fifth memory means 105 is identical with encryption of the challenging data stored in the fourth memory means 103 with the encryption key.

16. The device for authenticating user's access rights to resources of claim 14, wherein

the unique security characteristic information of the device 14 is a decryption key of a cipher function,
the verification device 10 comprises random number generation means 102 for generating a random number, sixth memory means 103 for

storing the generated random number and seventh memory means 122 for storing a seed for challenging data, and wherein

the random number generation means 102 stores the generated random number in the sixth memory means 103 while randomizing the seed for the challenging data stored in the seventh memory means 122 by executing predefined calculations to the random number stored in the sixth memory means 103 and the seed stored in the seventh memory means 122 and then storing the randomized seed as challenging data in the fourth memory means, and the verification means 106 of the verification device 10 de-randomizes the response stored in the fifth memory means 105 by executing predefined calculations to the random number stored in the sixth memory means 103 and the response stored in the fifth memory means 105, and then verifies the legitimacy of the de-randomized response by verifying that the de-randomized result is identical with decryption of the seed stored in the seventh memory means 122 with the decryption key which is the unique security characteristic information of the device 14.

17. The device for authenticating user's access rights to resources of claim 14, wherein

the unique security characteristic information of the device 14 is the signature key of a digital signature function, and
the verification device 10 comprises random number generation means 102 for generating a random number and storing the generated random number as challenging data in the fourth memory means, and wherein
the verification means 106 of the verification device 10 verifies the legitimacy of the response by verifying that the response stored in the fifth memory means 105 is identical with the digital signature for the challenging data stored in the fourth memory means, which is calculated with the signature key which is the unique security characteristic information of the device 14.

18. The device for authenticating user's access rights to resources of claim 15, wherein

the unique security characteristic information of the device 14 is the private key D of an RSA public key pair with a modulus n, and
the verification means 106 verifies the legitimacy of the response by verifying that the E-th power of the response R stored in the fifth memory means 105, where E denotes the public key associated with the private key D, is congruent with the challenging data C stored in the fourth memory means modulo n ($R^E \bmod n = C \bmod n$).

19. The device for authenticating user's access rights to resources of claim 16, wherein

the unique security characteristic information of the device 14 is the private key D of an RSA public key pair with a modulus n,
a seed C' for challenging data stored in the seventh memory means 122 is an RSA-encryption of data K with the public key E of the RSA public key pair ($DE \bmod \phi(n) = 1$, $C' = K^E \bmod n$),
a random number r generated by the random number generation means 102 is stored in the sixth memory means 103,
challenging data C generated and stored in the fourth memory means satisfies the relation $C = r^E C' \bmod n$, and
the verification means 106 verifies the legitimacy of the response R stored in the fifth memory means 105 by verifying that the quotient of R divided by r modulo n is congruent with the data K modulo n ($K \bmod n = r\text{-}1R \bmod n$).

20. The device for authenticating user's access rights to resources of claim 18 or 19, wherein

a proof support information t 13 stored in the third memory means 113 satisfies the relation $t = D - e + w\,\phi(n)$, where e denotes user unique identifying information 16 stored in the second memory means 115, w denotes a conflict-free random number determined dependent upon both n and e and $\phi(n)$ denotes the Euler number of n, and
the response generated by response generation means 116 is identical with the D-th power of challenging data C stored in the first memory means 111 modulo n ($R = C^D \bmod n$).

21. The device for authenticating user's access rights to resources of claim 20, wherein

the response generation means 116 further comprises:
third calculation means 112 for calculating the t-th power of challenging data C stored in the first memory means 111 modulo n ($C^t \bmod n$), where t denotes proof support information 13 stored in the third memory means 113;
fourth calculation means 114 for calculating the e-th power of the challenging data C modulo n ($C^e \bmod n$), where e denotes user unique identifying information 16 stored in the second memory means 115; and
fifth calculation means 116 for calculating a

response R by multiplying the result calculated by the third calculation means 112 by the result calculated by the fourth calculation means 114 modulo n ($R = C^{t}C^{e} \bmod n$).

22. The device for authenticating user's access rights to resources of claim 21, further comprising:

protect means 160 for preventing any data inside from being observed or being tampered with from the outside, confining the second memory means 115 and the fourth calculation means 114.

23. The device for authenticating user's access rights to resources of claim 18 or 19, wherein

proof support information t 13 stored in the third memory means 113 satisfies the relation $t = D + F(n, e)$, where e denotes user unique identifying information 16 stored in the second memory means 115, and F(x, y) denotes a two-variable collision-free function, and
a response generated by the response generation means 116 is identical with the D-th power of challenging data C stored in the first memory means 111 modulo n ($R = C^{D} \bmod n$).

24. The device for authenticating user's access rights to resources of claim 23, wherein

the response generation means 116 further comprises:
third calculation means 112 for calculating the t-th power of challenging data C stored in the first memory means 111 modulo n, where t denotes the proof support information 13 stored in the third memory means 113 ($C^{t} \bmod n$);
fourth calculation means 114 for calculating the F(n, e)-th power of the challenging data C modulo n ($C^{F(n,e)} \bmod n$), where e denotes the user unique identifying information 16 stored in the second memory means 115 and F(x, y) denotes a two-variable collision-free function; and
fifth calculation means 116 for calculating a response R by dividing the result calculated by the third calculation means 112 by the result calculated by the fourth calculation means 114 modulo n ($R = C^{t} C^{-F(n,e)} \bmod n$).

25. The device for authenticating user's access rights to resources of claim 24, further comprising:

protect means 160 for preventing any data inside from being observed or being tampered with from the outside, confining the second memory means 115 and the fourth calculation means 114.

26. The device for authenticating user's access rights to resources of claim 15, wherein

the unique security characteristic information of the device 14 is a key D of a Pohlig-Hellman key pair of a modulus p, and
the verification means 106 verifies the legitimacy of the response by verifying that the E-th power of the response R stored in the fifth memory means 105, where E denotes the counterpart key of the key D ($DE \bmod (p-1) = 1$), is congruent with the challenging data C stored in the fourth memory means modulo p ($R^{E} \bmod p = C \bmod p$).

27. The device for authenticating user's access rights to resources of claim 16, wherein

the unique security characteristic information of the device 14 is a key D of a Pohlig-Hellman key pair of a modulus p,
a seed C' for challenging data stored in the seventh memory means 422 is Pohlig-Hellman-encryption of data K with the counterpart key E of the key D ($DE \bmod (p-1) = 1$, $C' = K^{E} \bmod p$),
a random number r generated by the random number generation means 402 is stored in the sixth memory means 403,
challenging data C stored in the fourth memory means satisfies the relation $C = r^{E}C' \bmod p$, and
the verification means 106 verifies the legitimacy of the response R stored in the fifth memory means 405 by verifying that the quotient of R divided by r modulo p is congruent with the data K modulo p ($K \bmod p = r^{-1}R \bmod p$).

28. The device for authenticating user's access rights to resources of claim 26 or 27, wherein

proof support information t 13 stored in the third memory means 413 satisfies the relation $t = D + F(p, e)$, where e denotes the user unique identifying information 16 stored in the second memory means 415, and F(x, y) denotes a two-variable collision-free function, and
a response generated by the response generation means 416 is identical with the D-th power of challenging data C stored in the first memory means 411 modulo p ($R = C^{D} \bmod p$).

29. The device for authenticating user's access rights to resources of claim 28, wherein

the response generation means 416 further

comprises:

third calculation means 412 for calculating the t-th power of challenging data C stored in the first memory means 411 modulo p, where t denotes the proof support information 13 stored in the third memory means 413 (C^t mod p);

fourth calculation means 414 for calculating the F(p, e)-th power of the challenging data C modulo p ($C^{F(p,e)}$ mod p), where e denotes the user unique identifying information 16 stored in the second memory means 415 and F(x, y) denotes a two-variable collision-free function; and

fifth calculation means 416 for calculating a response R by dividing the result calculated by the third calculation means 412 by the result calculated by the fourth calculation means 414 modulo p ($R = C^t C^{-F(p,e)}$ mod p).

30. The device for authenticating user's access rights to resources of claim 29, further comprising:

protect means 160 for preventing any data inside from being observed or being tampered with from the outside, confining the second memory means 415 and the fourth calculation means 414.

31. The device for authenticating user's access rights to resources of claim 16, wherein

the unique security characteristic information of the device 14 is the private key X of an ElGamal public key pair with a modulus p and a generator G,

the public key Y corresponding to X is the X-th power of G modulo p ($Y = G^X$ mod p),

u denotes the z-th power of the modulo p ($u = G^z$ mod p) for a random number z,

K' denotes the product modulo p of the z-th power of Y modulo p and a data K ($K' = Y^z K$ mod p),

the seventh memory means 522 retains the pair of u and K',

a random number r generated by the random generation means 602 is stored in the sixth memory means 603,

C denotes the product modulo p of K' and r ($C = rK'$ mod p),

the fourth memory means retains the pair C and u, and

the verification means 106 verifies the legitimacy of the response R stored in the fifth memory means 505 by verifying that the quotient of R divided by r modulo p is congruent with K modulo p ($K \bmod p = r^{-1} R \bmod p$).

32. The device for authenticating user's access rights to resources of claim 31, wherein

proof support information t 13 stored in the third memory means 513 satisfies the relation $t = D + F(p, e)$, where e denotes the user unique identifying information 16 stored in the second memory means 515 and F(x, y) denotes a two-variable collision-free function, and

a response R generated by the response generation means 516 is identical with the quotient of C divided by X-th power of u modulo p ($R = u^{-X} C$ mod p), where the pair C and u is the challenging data stored in the first memory means 511.

33. The device for authenticating user's access rights to resources of claim 32, wherein

the response generation means 516 further comprises:

third calculation means 512 for calculating the t-th power of the component u of the challenging data pair stored in the first memory means 511 modulo p, where t denotes proof support information stored in the third memory means 513 (ut mod p);

fourth calculation means 514 for calculating the F(p, e)-th power of u modulo p ($u^{F(p,e)}$ mod p), where e denotes the user unique identifying information 16 stored in the second memory means 515 and F(x, y) denotes a two-variable collision-free function; and

fifth calculation means 516 for calculating a response R by dividing the product of the other component C of the challenging data pair and the result calculated by the fourth calculation means 514 by the result calculated by the third calculation means 512 modulo p. ($R = Cu^{F(n,e)} u^{-t}$ mod p).

34. The device for authenticating user's access rights to resources of claim 33, further comprising:

protect means 160 for preventing any data inside from being observed or being tampered with from the outside, confining the second memory means 515 and the fourth calculation means 514.

35. The device for authenticating user's access rights to resources of claim 17, wherein

the unique security characteristic information of the device 14 is the signature key X of an ElGamal public key pair with a modulus p and a generator G,

the public key Y corresponding to X is the X-th power of G modulo p ($Y = G^X$ mod p),

a response stored in the fifth memory means 605 is a pair of R and S, and

the verification means 606 verifies the legitimacy of the response R stored in the fifth memory means 605 by verifying that the C-th power of G for the challenging data C stored in the fourth memory means is congruent modulo p with the product of the R-th power of Y and the S-th power of R ($G^C \bmod p = Y^R R^S \bmod p$).

36. The device for authenticating user's access rights to resources of claim 35, wherein

proof support information t 13 stored in the third memory means 613 satisfies the relation $t = D + F(p, e)$, where e denotes the user unique identifying information 16 stored in the second memory means 616, and F(x, y) denotes a two-variable collision-free function, and

the response generation means 116 generates a response pair R and S by carrying out the following steps of:

generating a random number k;

calculating R as the k-th power of G modulo p ($R = G^k \bmod p$); and

calculating S according to the relation $S = (C - RX)\, k^{-1} \bmod (p-1)$.

37. The device for authenticating user's access rights to resources of claim 36, further comprising:

protect means 160 for preventing any data inside from being observed or being tampered with from the outside, confining the second memory means 616 and the fourth calculation means 614.

38. The device for authenticating user's access rights to resources of claim 4, wherein

the user unique identifying information 16 stored in the second memory means 715 is a decryption key of a cipher function,

the proof support information 13 stored in the third memory means 713 is an encryption of the unique security characteristic information of the device with the encryption key corresponding the decryption key, and

the first calculation means 712 calculates the unique security characteristic information of the device 14 by decrypting the proof support information stored in the third memory means 713 with the decryption key stored in the second memory means 715.

39. The device for authenticating user's access rights to resources of claim 38, wherein

the cipher function is of the asymmetric key cryptography, and

the user unique identifying information 16 is a component of the key pair of the cipher function.

40. The device for authenticating user's access rights to resources of claim 39, wherein

the cipher function is of the public key cryptography, and

the user unique identifying information 16 is the private key of the public key pair of the cipher function.

41. The device for authenticating user's access rights to resources of claim 38, wherein

the cipher function is of the symmetric key cryptography, and

the user unique identifying information 16 is the common secret key of the cipher function.

42. The device for authenticating user's access rights to resources of claim 8 or 16, wherein

the verification device 10 further comprises:

eighth memory means 310a for storing a clear data encryption of which is the challenging data or the seed for challenging data stored in the first memory means 111; and

comparison means 310b for examining whether the clear data stored in the eighth memory means 310a is identical with data inputted to the comparison means 310b, and wherein

the verification means 106 feeds the response or the de-randomized value of the response stored in the fifth memory means 105 to the comparison means 310b, receives the answer from the comparison means 310b, and thereby the verification means 106 verifies the legitimacy of the response if and only if the received answer shows that the clear data stored in the eighth memory means 310a is identical with the data inputted to the comparison means 310b.

43. The device for authenticating user's access rights to resources of claim 8 or 16, wherein

the verification device 10 further comprises:

ninth memory means 310a for storing a value obtained by applying a one-way function to clear data encryption of which is the challenging data or the seed for challenging data stored in the seventh memory means 122;

sixth calculation means 310c for outputting a value calculated by applying the one-way func-

tion to an inputted data; and

comparison means 310b for examining whether the value stored in the ninth memory means 310a is identical with data inputted to the comparison means 310b, and wherein

the verification means 106 feeds the response or the de-randomized value of the response to the sixth calculation means 310c, receives a result from the sixth calculation means 310c, feeds the result to the comparison means 310b and receives an answer from the comparison means 310b, and thereby the verification means 106 verifies the legitimacy of the response if and only if the received answer shows that the result of the calculation by the sixth calculation means 310c is identical with the data stored in the ninth memory means 310a.

44. The device for authenticating user's access rights to resources of claim 8 or 16, wherein

the verification device 10 further comprises:

program execution means 310 for executing code of a program encryption of which is the challenging data stored in the seventh memory means 122, and wherein

the verification means 106 feeds the response stored in the fifth memory means 105 as program code to the program execution means 310, and

the program execution means 310 correctly functions if and only if the response generation means 116 correctly decrypts the challenging data which is an encryption of the code of the program, that is, the encryption of the program is correctly decrypted.

45. The device for authenticating user's access rights to resources of claim 8 or 16, wherein

the verification device 10 further comprises:

program execution means 310;

program storing means 310g; and

program decryption means 310h, and wherein

the program storing means 310g stores code of a program a part or all of which is encrypted,

an encryption of the decryption key for the partial or whole encrypted program code is the challenging data stored in the seventh memory means 122,

the verification means 106 feeds the response to the program decryption means 310h,

the program decryption means 310h decrypts the program stored in the program storing means 310g with the response as a decryption key, and

the program execution means 310 correctly executes the decrypted program if and only if the response generation means 116 correctly decrypts the challenging data, that is, the decryption key for decrypting the encryption of the program is correctly decrypted.

46. The device for authenticating user's access rights to resources of claim 14, wherein

the proving device 11 and the verification device 10 are installed in a box material, and

the verification device 10 transfers the challenging data 18 stored in the fourth memory means to the first memory means 111 of the proving device 11 and the proving device 11 transfers the response 19 generated by the response generation means 116 to the fifth memory means 105 of the verification device 10 without using a communication network outside of the box material.

47. A method for authenticating user's access rights to resources by verifying the legitimacy of a response generated from challenging data for proving the user's access rights, comprising:

a step for storing the challenging data;

a step for storing unique identifying information of the user;

a step for storing proof support information which is a result of predetermined computations to the unique identifying information of the user and unique security characteristic information;

a step for generating a response by executing predetermined computations to the challenging data, the unique identifying information of the user and the proof support information; and

a step for verifying the legitimacy of the response by verifying that the response, the challenging data and the unique security characteristic information satisfy a specific predefined relation.

48. A computer program product for use with a computer, the computer program product comprising:

a computer usable medium having computer readable program code means embodied in the medium for causing the computer to authenticate user's access rights to resources by verifying the legitimacy of a response 19 generated from challenging data 18 for proving the user's access rights, the computer program product having:

computer readable program code means for causing the computer to store the challenging data 18;

computer readable program code means for causing the computer to store unique identify-

ing information of the user 16;

computer readable program code means for causing the computer to store proof support information 13 which is a result of predetermined computations to the unique identifying information of the user 16 and unique security characteristic information 14;

computer readable program code means for causing the computer to generate a response 19 by executing a predetermined computations to the challenging data 18, the unique identifying information of the user 16 and the proof support information 13; and

computer readable program code means for causing the computer to verify the legitimacy of the response 19 by verifying that the response 19, the challenging data 18 and the unique security characteristic information 14 satisfy a specific predefined relation.

49. A computer program product for use with a computer, the computer program product comprising:

a computer usable medium having computer readable program code means embodied in the medium for causing the computer to generate a response 19 from challenging data 18, the legitimacy of which is to be verified for authenticating user's access rights, the computer program product having:

computer readable program code means for causing the computer to store the challenging data 18;

computer readable program code means for causing the computer to store unique identifying information of the user 16;

computer readable program code means for causing the computer to store proof support information 13 which is a result of predetermined computations to the unique identifying information of the user 16 and unique security characteristic information 14; and

computer readable program code means for causing the computer to generate a response 19 by executing predetermined computations to the challenging data 18, the unique identifying information of the user 16 and the proof support information 13.

50. A program execution control device for authenticating user's access rights to resources by verifying the legitimacy of a response generated from challenging data for proving the user's access rights and controlling execution of a program based on the authentication of the user's access rights, comprising:

first memory means 111 for storing challenging data 18;

second memory means 115 for storing unique identifying information of the user 16;

third memory means 113 for storing proof support information 13 which is a result of predetermined computations to the unique identifying information of the user 16 and unique security characteristic information of the device 14;

response generation means 116 for generating a response 19 by executing predetermined computations to the challenging data 18, the unique identifying information of the user 16 and the proof support information 13;

verification means 106 for verifying the legitimacy of the response 19 by verifying that the response 19, the challenging data 18 and the unique security characteristic information 14 satisfy a specific predefined relation; and

continuation means for continuing execution of the program if the legitimacy of the response is verified.

51. An information processing apparatus for authenticating user's access rights to specific information processing resources by verifying the legitimacy of a response 19 generated for proving the user's access rights and permitting access to the specific information processing resources, comprising:

first memory means 111 for storing challenging data 18;

second memory means 115 for storing unique identifying information of the user 16;

third memory means 113 for storing proof support information 13 which is a result of predetermined computations to the unique identifying information of the user 16 and unique security characteristic information 14;

response generation means 116 for generating a response 19 by executing predetermined computations to the challenging data 18, the unique identifying information of the user 16 and the proof support information 13;

verification means 106 for verifying the legitimacy of the response 19 by verifying that the response 19, the challenging data 18 and the unique security characteristic information 14 satisfy a specific predefined relation; and

permission means for permitting access to the specific information processing resources if the legitimacy of the response is verified.

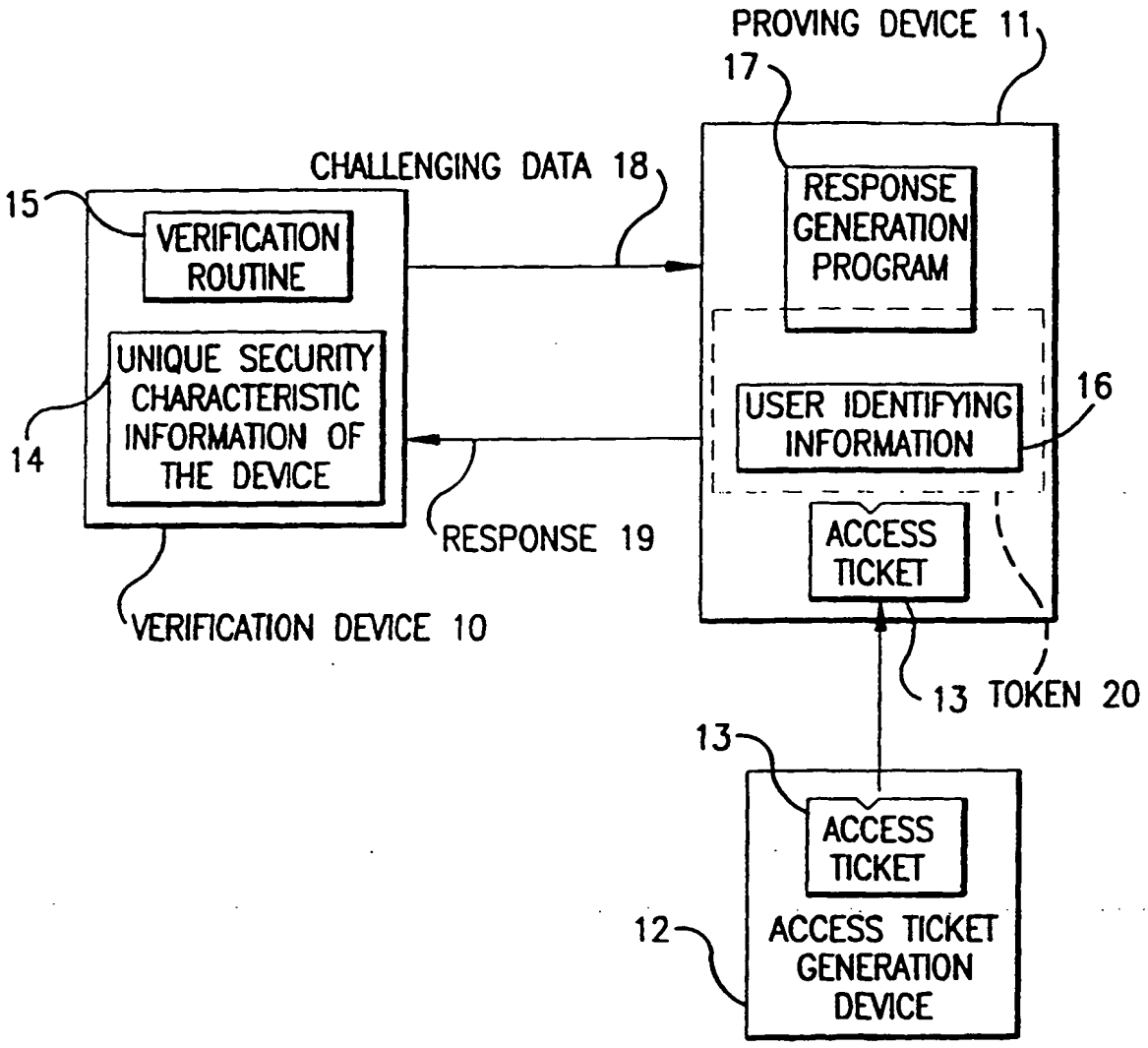

PROVING DEVICE 11
17
CHALLENGING DATA 18
15
VERIFICATION ROUTINE
RESPONSE GENERATION PROGRAM
UNIQUE SECURITY CHARACTERISTIC INFORMATION OF THE DEVICE
14
USER IDENTIFYING INFORMATION
16
ACCESS TICKET
RESPONSE 19
VERIFICATION DEVICE 10
13 TOKEN 20
13
ACCESS TICKET
12
ACCESS TICKET GENERATION DEVICE

FIG.1

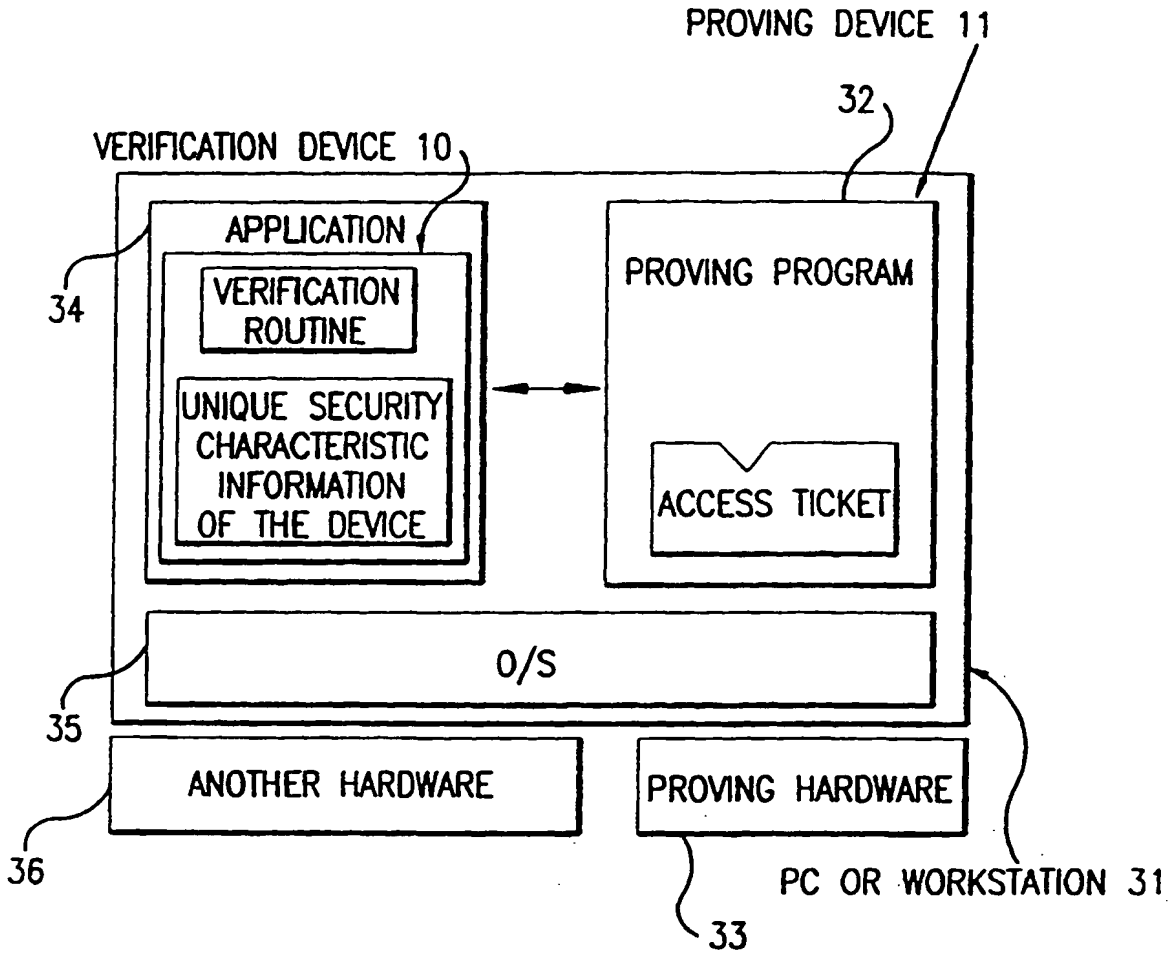

PROVING DEVICE 11
32
VERIFICATION DEVICE 10
APPLICATION
VERIFICATION ROUTINE
UNIQUE SECURITY CHARACTERISTIC INFORMATION OF THE DEVICE
34
PROVING PROGRAM
ACCESS TICKET
O/S
35
ANOTHER HARDWARE
36
PROVING HARDWARE
33
PC OR WORKSTATION 31

FIG.2

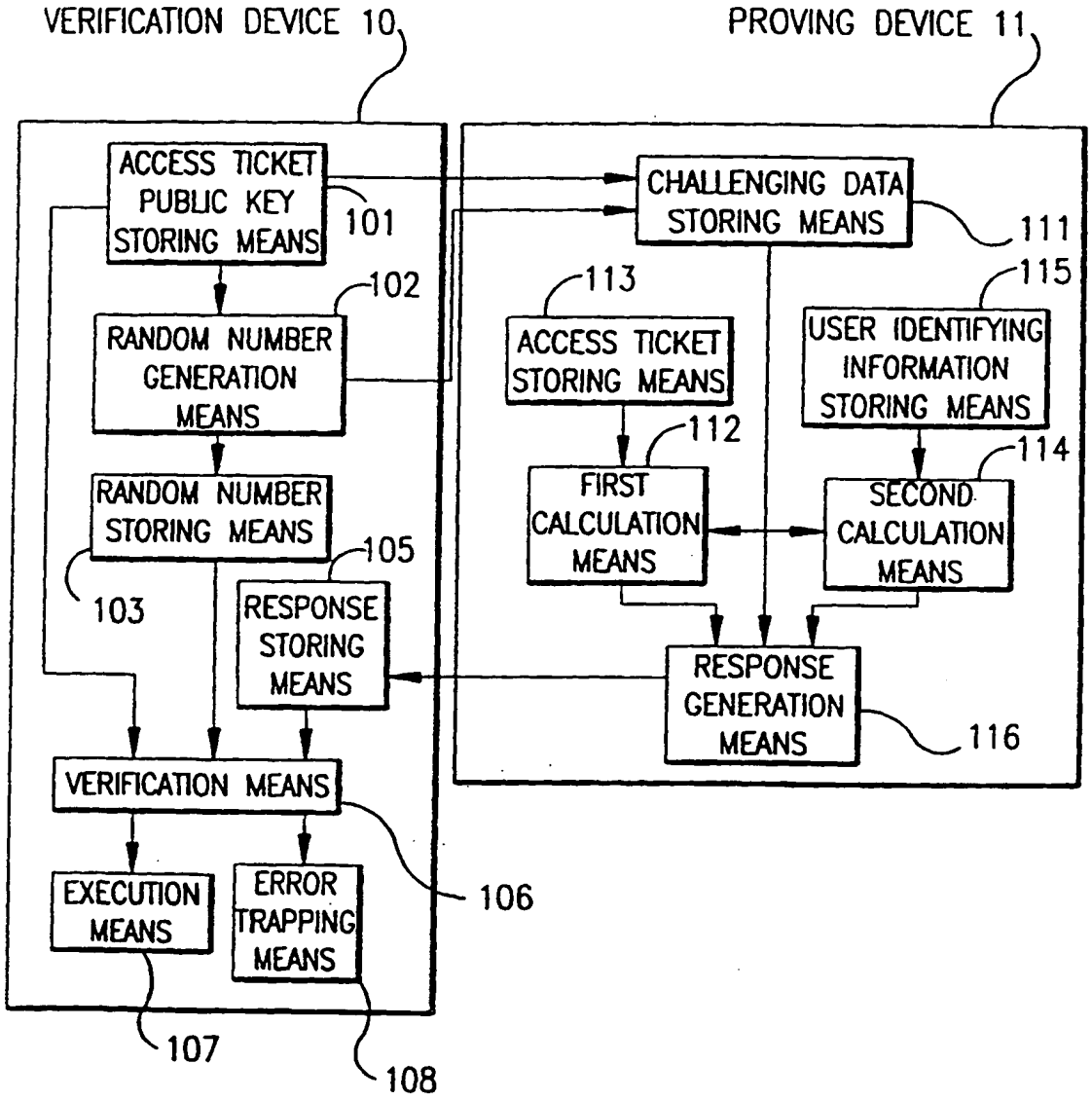

VERIFICATION DEVICE 10
PROVING DEVICE 11
ACCESS TICKET PUBLIC KEY STORING MEANS
101
RANDOM NUMBER GENERATION MEANS
102
RANDOM NUMBER STORING MEANS
103
RESPONSE STORING MEANS
105
VERIFICATION MEANS
106
EXECUTION MEANS
ERROR TRAPPING MEANS
107
108
CHALLENGING DATA STORING MEANS
111
ACCESS TICKET STORING MEANS
113
FIRST CALCULATION MEANS
112
USER IDENTIFYING INFORMATION STORING MEANS
115
SECOND CALCULATION MEANS
114
RESPONSE GENERATION MEANS
116

FIG.3

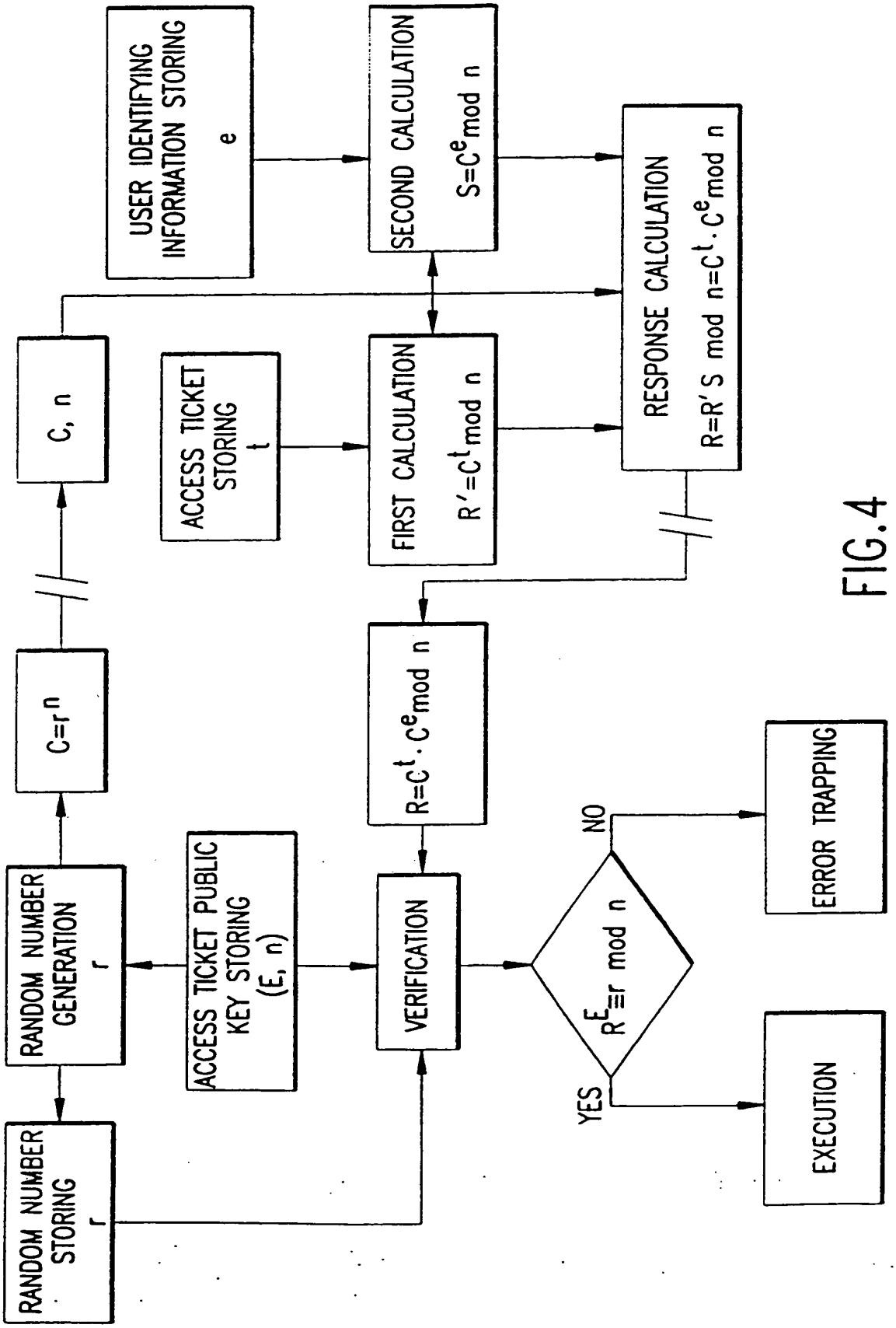

USER IDENTIFYING INFORMATION STORING
e
SECOND CALCULATION
$S=C^e \bmod n$
C, n
ACCESS TICKET STORING
t
FIRST CALCULATION
$R'=C^t \bmod n$
RESPONSE CALCULATION
$R=R'S \bmod n = C^t \cdot C^e \bmod n$
C=r^n
$R=C^t \cdot C^e \bmod n$
RANDOM NUMBER GENERATION
r
ACCESS TICKET PUBLIC KEY STORING
(E, n)
VERIFICATION
$R^E \equiv r \bmod n$
NO
YES
ERROR TRAPPING
EXECUTION
RANDOM NUMBER STORING
r

FIG.4

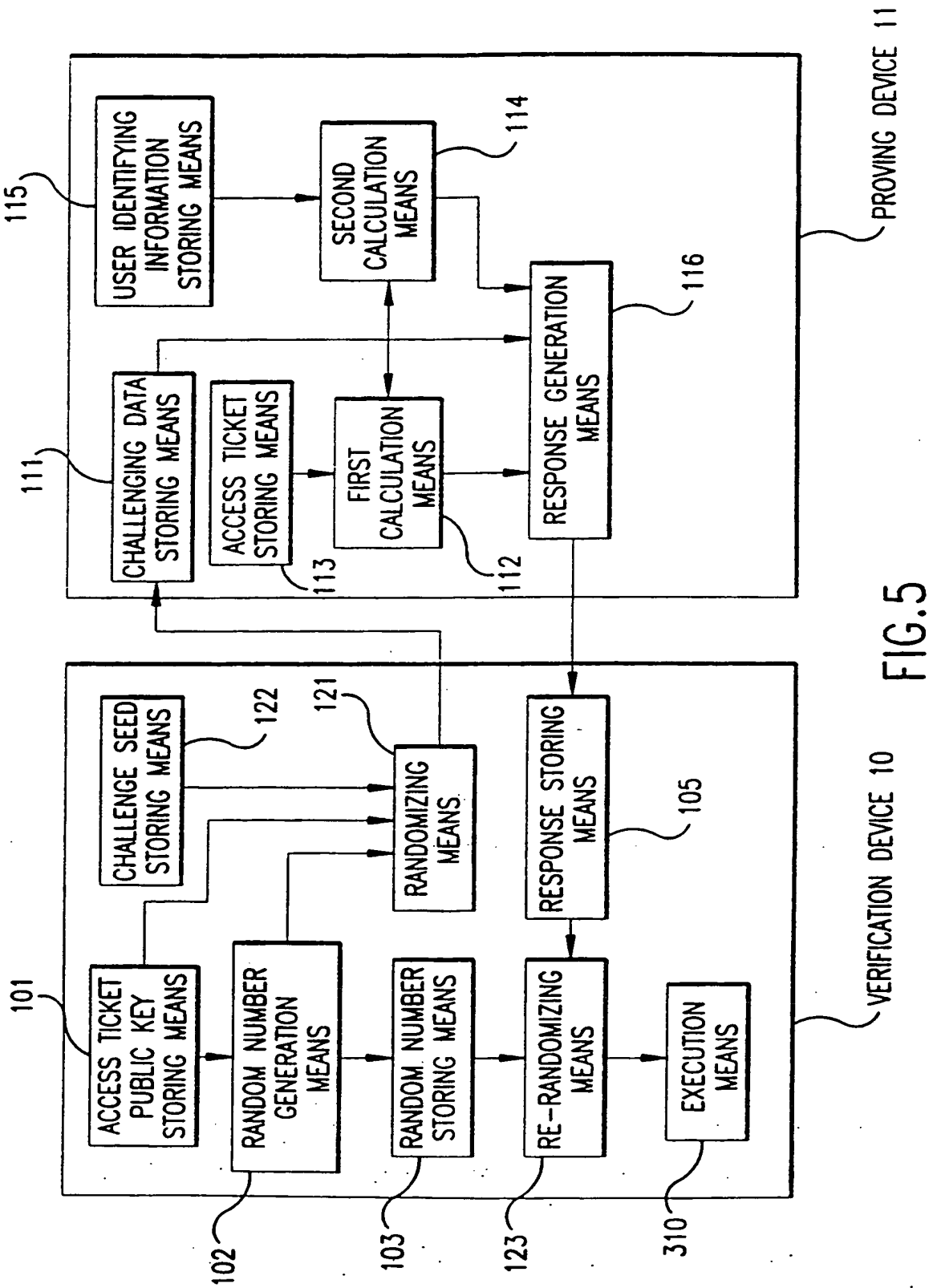

PROVING DEVICE 11
USER IDENTIFYING INFORMATION STORING MEANS
115
SECOND CALCULATION MEANS
114
RESPONSE GENERATION MEANS
116
CHALLENGING DATA STORING MEANS
111
ACCESS TICKET STORING MEANS
113
FIRST CALCULATION MEANS
112
VERIFICATION DEVICE 10
CHALLENGE SEED STORING MEANS
122
121
RANDOMIZING MEANS
RESPONSE STORING MEANS
105
101
ACCESS TICKET PUBLIC KEY STORING MEANS
RANDOM NUMBER GENERATION MEANS
RANDOM NUMBER STORING MEANS
RE-RANDOMIZING MEANS
EXECUTION MEANS
102
103
123
310

FIG.5

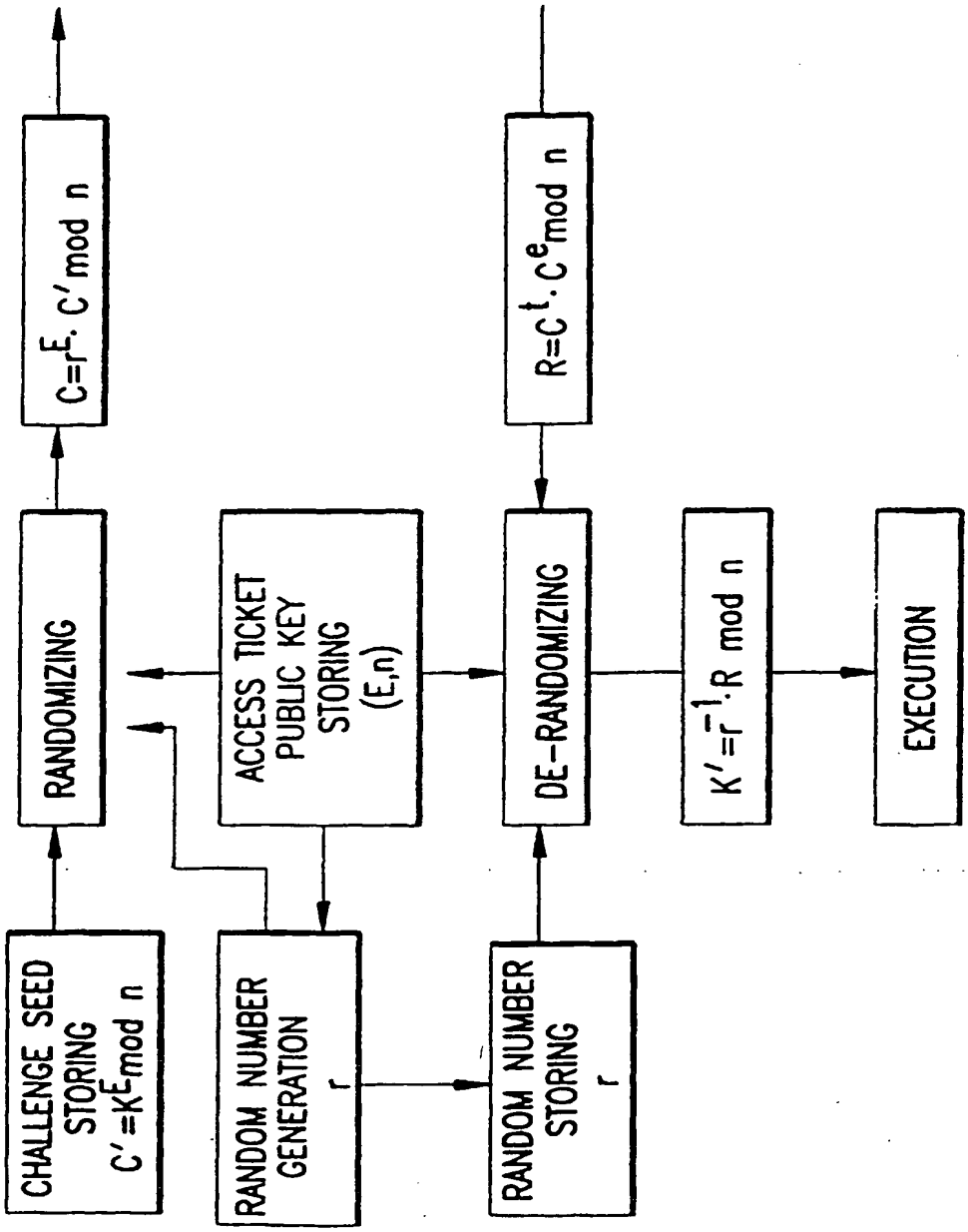

CHALLENGE SEED STORING C'=K^E mod n
RANDOMIZING
C=r^E. C' mod n
RANDOM NUMBER GENERATION r
ACCESS TICKET PUBLIC KEY STORING (E,n)
RANDOM NUMBER STORING r
R=C^t. C^e mod n
DE-RANDOMIZING
K'=r^-1.R mod n
EXECUTION

FIG.6

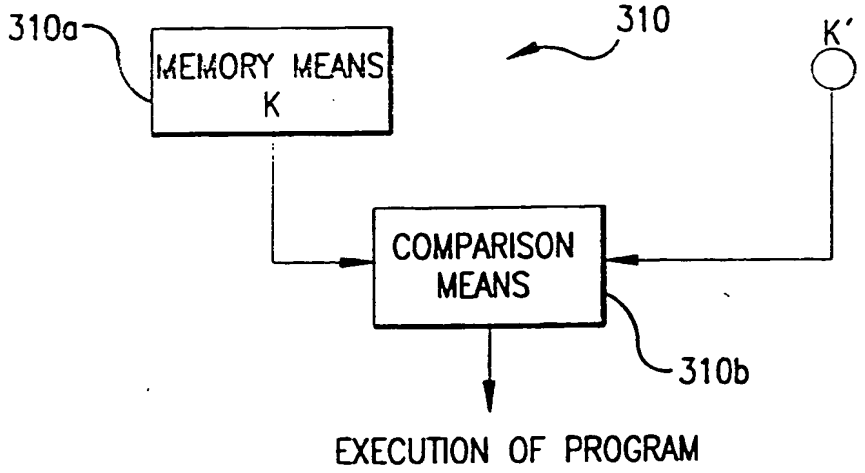

310a
MEMORY MEANS
K
310
K'
COMPARISON
MEANS
310b
EXECUTION OF PROGRAM

FIG.7

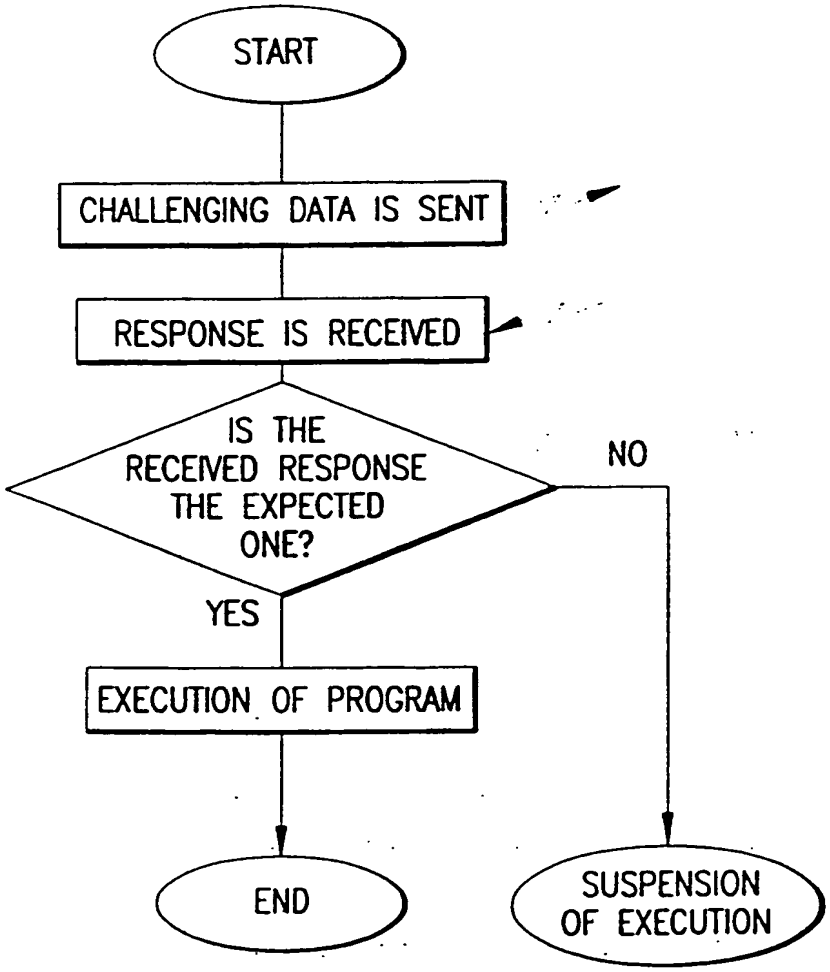

START
CHALLENGING DATA IS SENT
RESPONSE IS RECEIVED
IS THE
RECEIVED RESPONSE
THE EXPECTED
ONE?
NO
YES
EXECUTION OF PROGRAM
END
SUSPENSION
OF EXECUTION

FIG.8

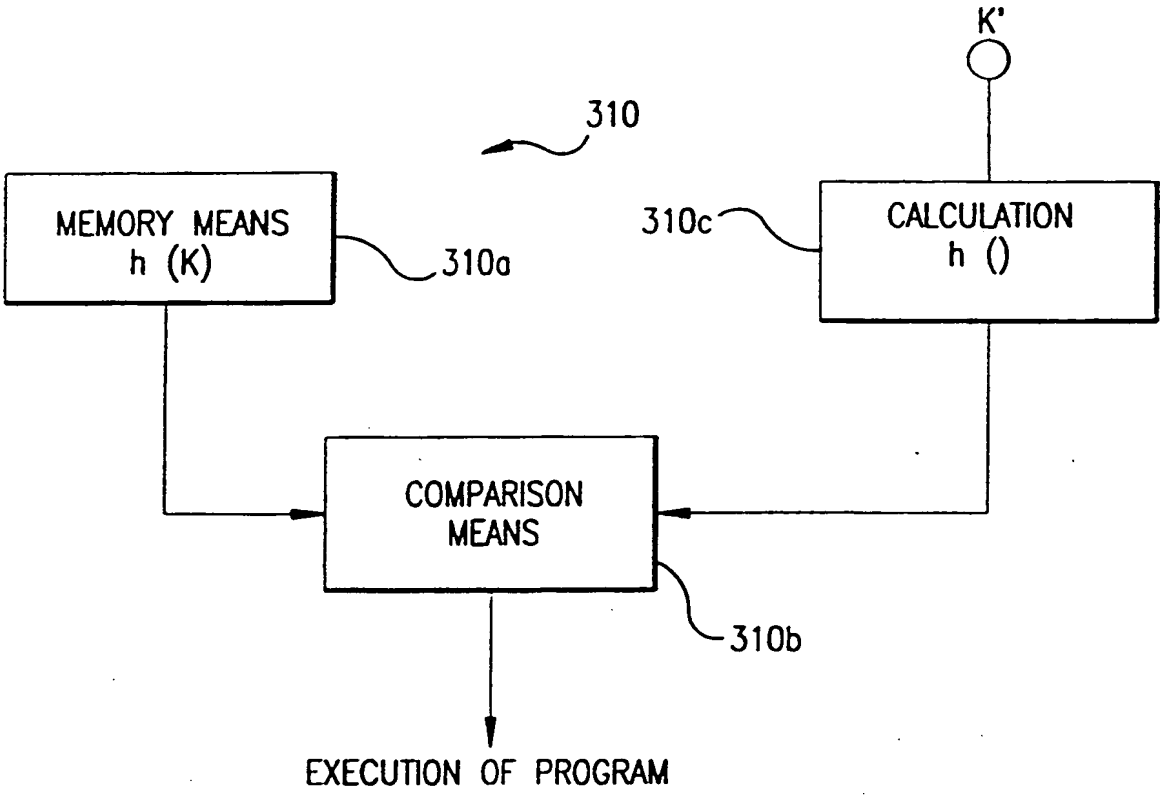

K'
310
MEMORY MEANS
h (K)
310a
310c
CALCULATION
h ()
COMPARISON
MEANS
310b
EXECUTION OF PROGRAM

FIG.9

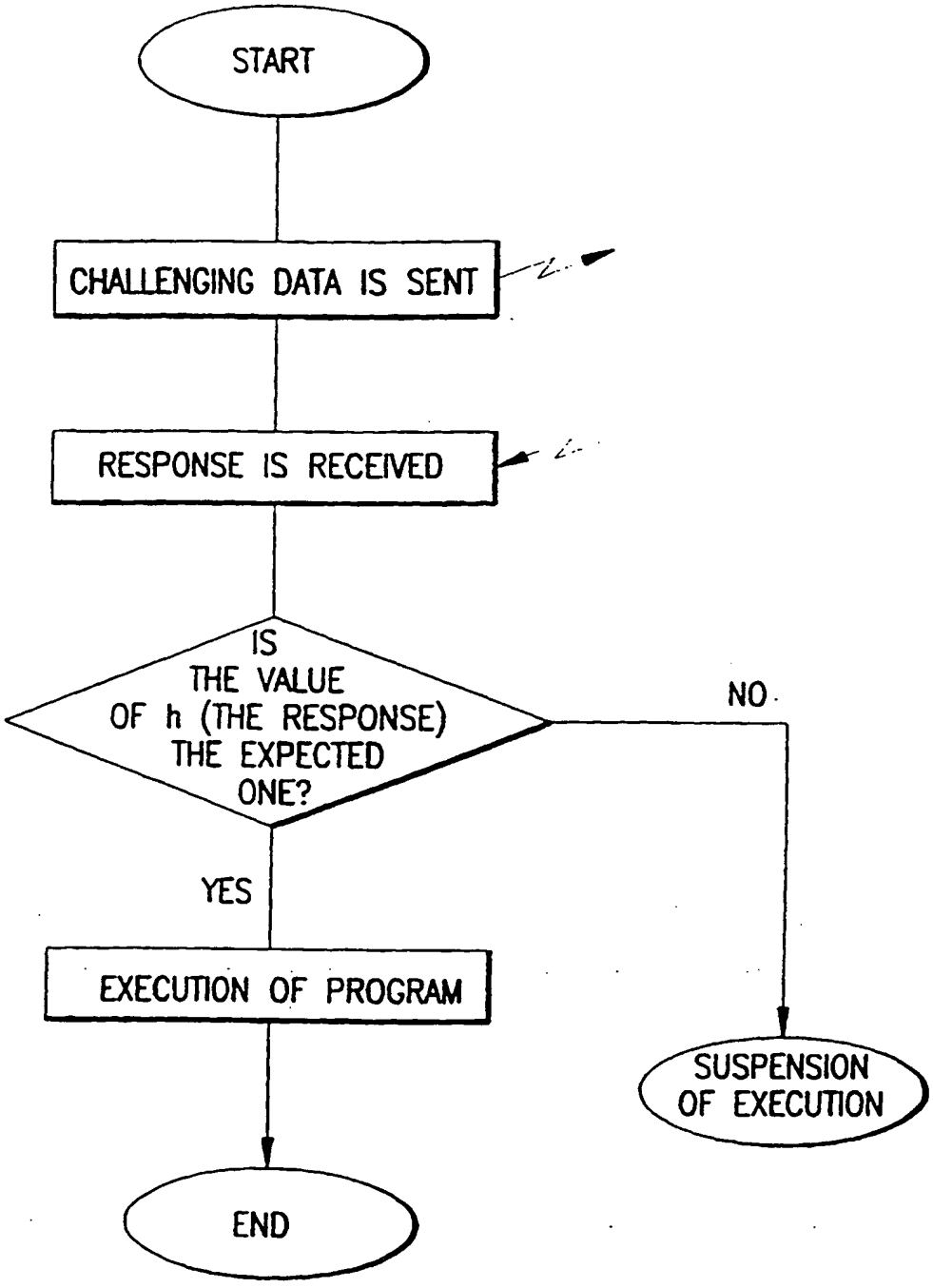

START
CHALLENGING DATA IS SENT
RESPONSE IS RECEIVED
IS THE VALUE OF h (THE RESPONSE) THE EXPECTED ONE?
NO
YES
EXECUTION OF PROGRAM
SUSPENSION OF EXECUTION
END

FIG.10

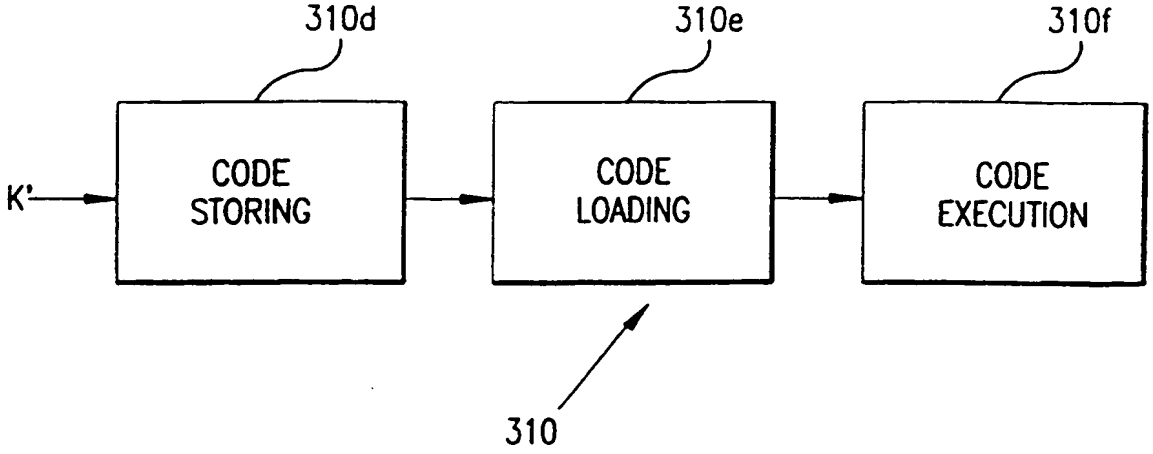

310d
310e
310f
K'
CODE STORING
CODE LOADING
CODE EXECUTION
310

FIG.11

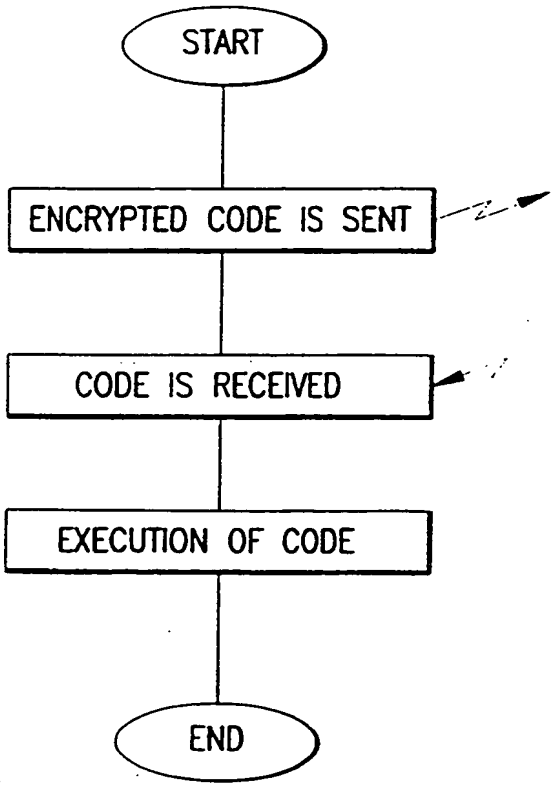

START
ENCRYPTED CODE IS SENT
CODE IS RECEIVED
EXECUTION OF CODE
END

FIG.12

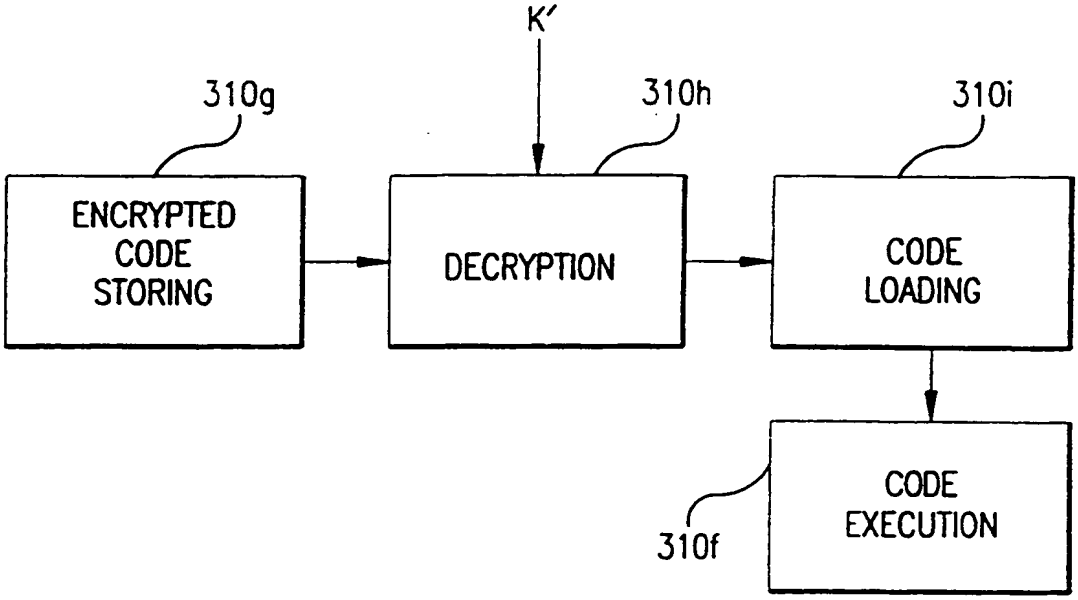

K'
310g
310h
310i
ENCRYPTED CODE STORING
DECRYPTION
CODE LOADING
CODE EXECUTION
310f

FIG.13

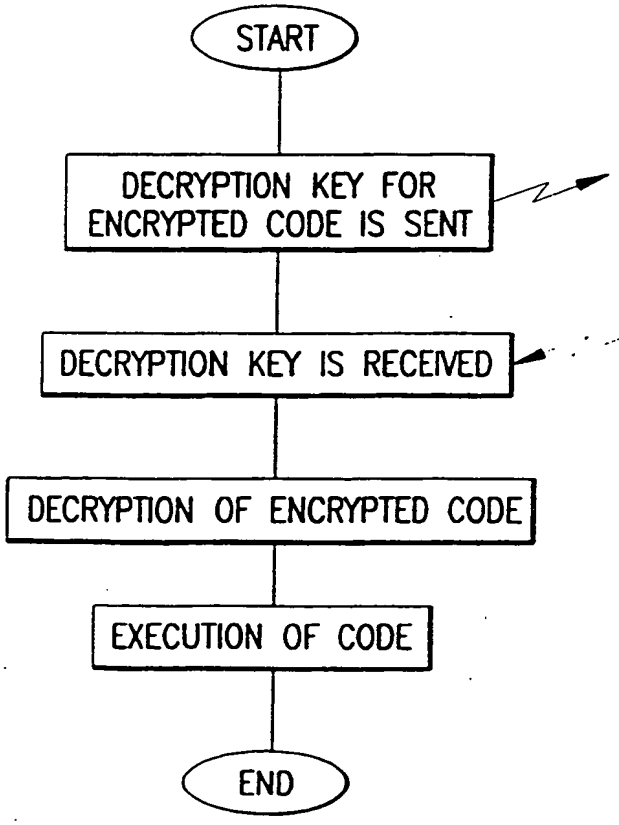

START
DECRYPTION KEY FOR ENCRYPTED CODE IS SENT
DECRYPTION KEY IS RECEIVED
DECRYPTION OF ENCRYPTED CODE
EXECUTION OF CODE
END

FIG.14

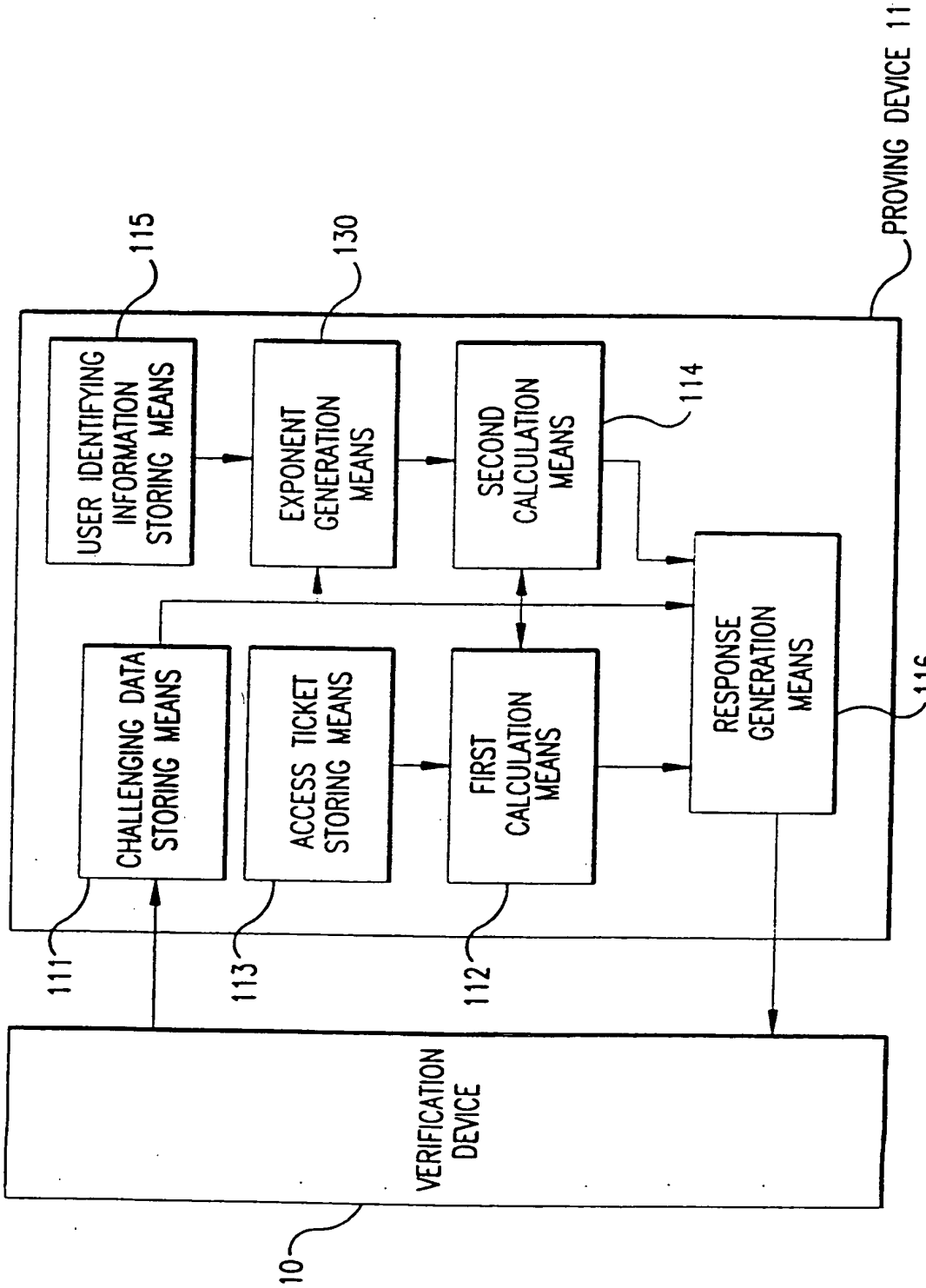

PROVING DEVICE 11
115
130
USER IDENTIFYING INFORMATION STORING MEANS
EXPONENT GENERATION MEANS
SECOND CALCULATION MEANS
114
CHALLENGING DATA STORING MEANS
ACCESS TICKET STORING MEANS
FIRST CALCULATION MEANS
RESPONSE GENERATION MEANS
116
111
113
112
VERIFICATION DEVICE
10

FIG.15

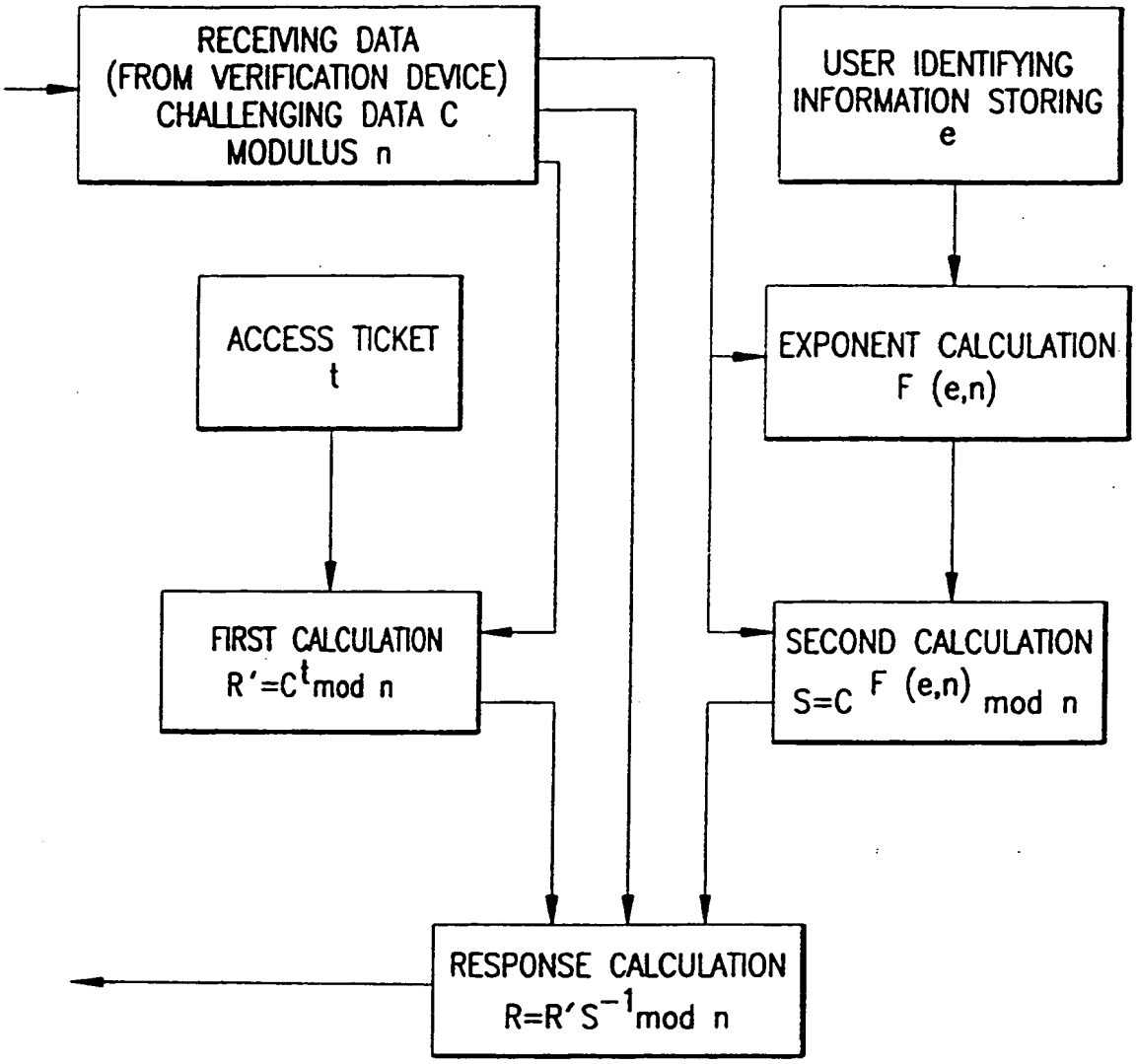

RECEIVING DATA
(FROM VERIFICATION DEVICE)
CHALLENGING DATA C
MODULUS n
USER IDENTIFYING INFORMATION STORING
e
ACCESS TICKET
t
EXPONENT CALCULATION
F (e,n)
FIRST CALCULATION
R'=C^t mod n
SECOND CALCULATION
S=C^F(e,n) mod n
RESPONSE CALCULATION
R=R'S^-1 mod n

FIG.16

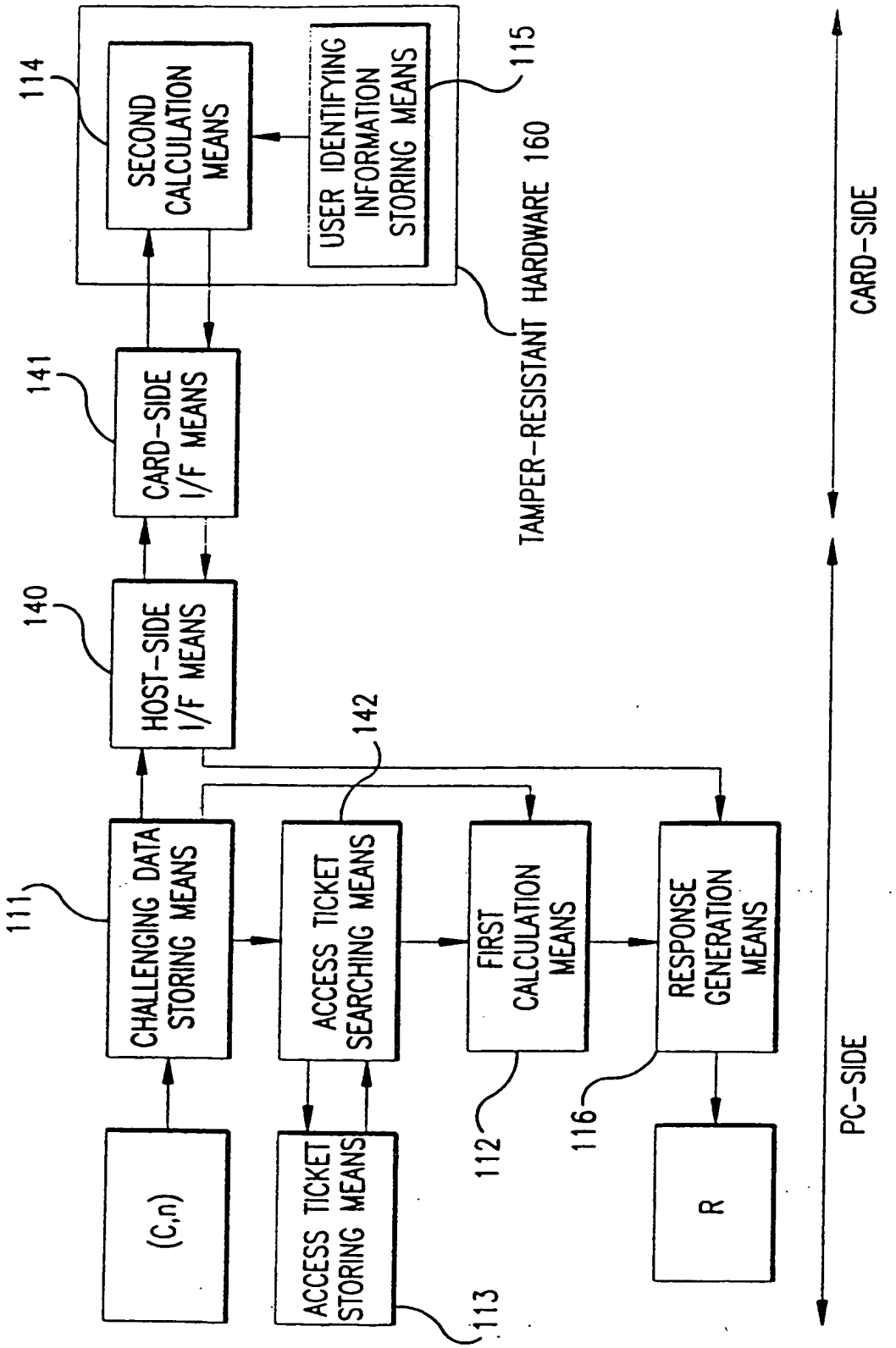

114
SECOND CALCULATION MEANS
USER IDENTIFYING INFORMATION STORING MEANS
115
TAMPER-RESISTANT HARDWARE 160
141
CARD-SIDE I/F MEANS
140
HOST-SIDE I/F MEANS
142
111
CHALLENGING DATA STORING MEANS
ACCESS TICKET SEARCHING MEANS
FIRST CALCULATION MEANS
RESPONSE GENERATION MEANS
(C,n)
ACCESS TICKET STORING MEANS
113
112
116
R
CARD-SIDE
PC-SIDE

FIG.17

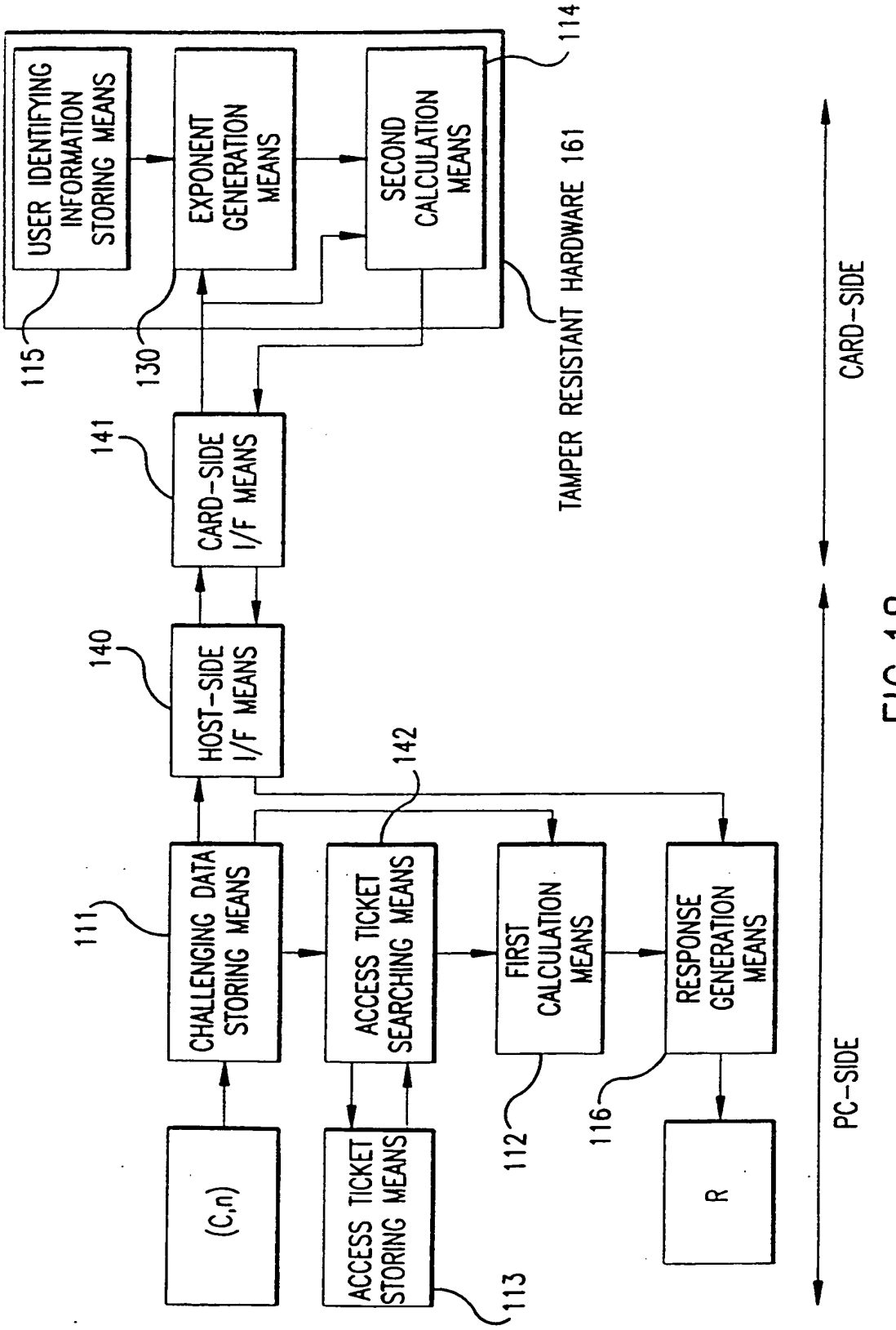

USER IDENTIFYING INFORMATION STORING MEANS
EXPONENT GENERATION MEANS
SECOND CALCULATION MEANS
114
TAMPER RESISTANT HARDWARE 161
115
130
141
CARD-SIDE I/F MEANS
140
HOST-SIDE I/F MEANS
142
111
CHALLENGING DATA STORING MEANS
ACCESS TICKET SEARCHING MEANS
FIRST CALCULATION MEANS
RESPONSE GENERATION MEANS
(C,n)
ACCESS TICKET STORING MEANS
113
112
116
R
CARD-SIDE
PC-SIDE

FIG.18

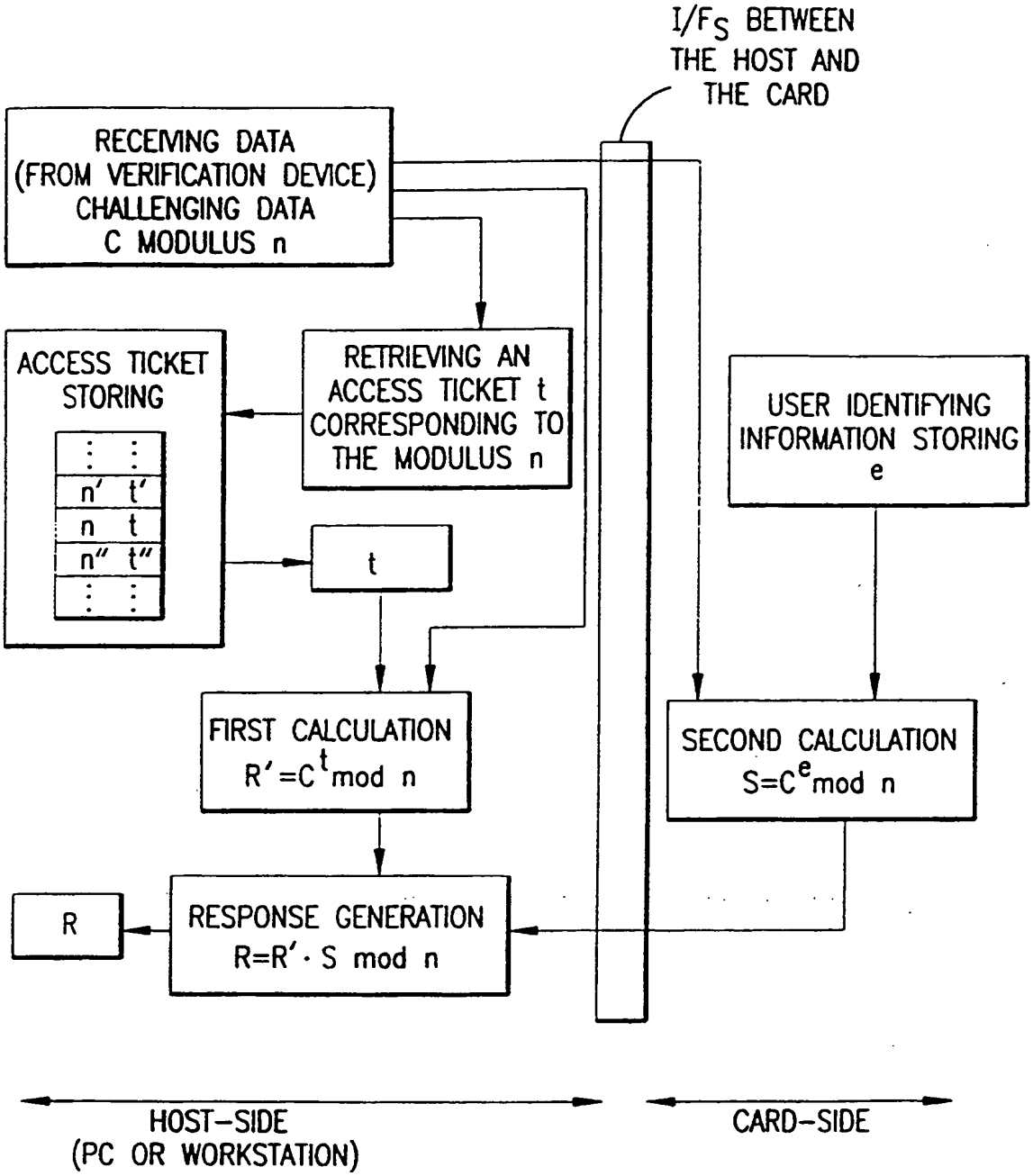

I/F$_S$ BETWEEN THE HOST AND THE CARD
RECEIVING DATA (FROM VERIFICATION DEVICE) CHALLENGING DATA C MODULUS n
ACCESS TICKET STORING
n' t'
n t
n'' t''
RETRIEVING AN ACCESS TICKET t CORRESPONDING TO THE MODULUS n
t
USER IDENTIFYING INFORMATION STORING e
FIRST CALCULATION $R'=C^t \bmod n$
SECOND CALCULATION $S=C^e \bmod n$
R
RESPONSE GENERATION $R=R' \cdot S \bmod n$
HOST-SIDE (PC OR WORKSTATION)
CARD-SIDE

FIG.19

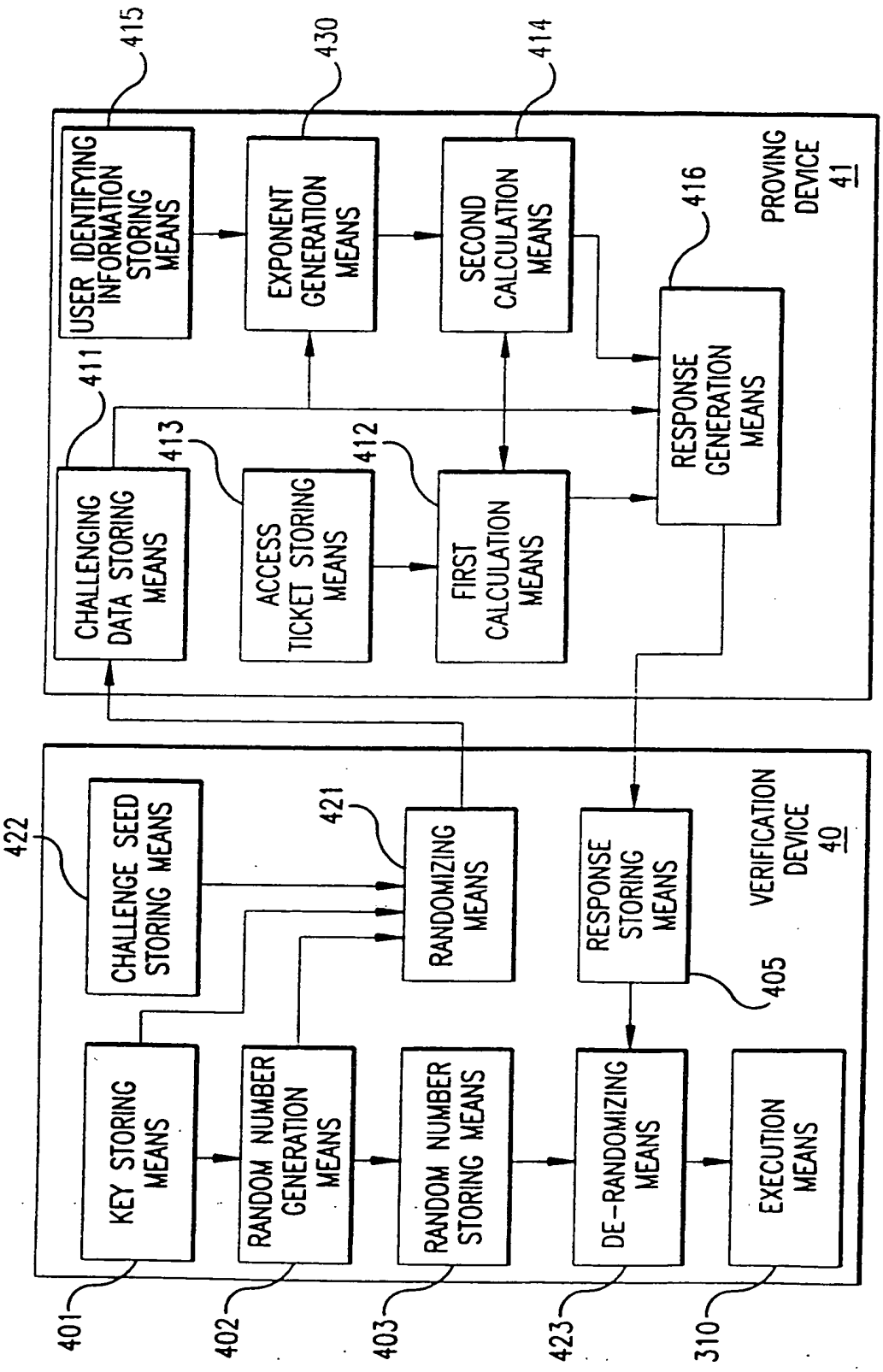

PROVING DEVICE 41
USER IDENTIFYING INFORMATION STORING MEANS
EXPONENT GENERATION MEANS
SECOND CALCULATION MEANS
RESPONSE GENERATION MEANS
CHALLENGING DATA STORING MEANS
ACCESS TICKET STORING MEANS
FIRST CALCULATION MEANS
VERIFICATION DEVICE 40
CHALLENGE SEED STORING MEANS
RANDOMIZING MEANS
RESPONSE STORING MEANS
KEY STORING MEANS
RANDOM NUMBER GENERATION MEANS
RANDOM NUMBER STORING MEANS
DE-RANDOMIZING MEANS
EXECUTION MEANS
415
430
414
416
411
413
412
422
421
405
401
402
403
423
310

FIG.20

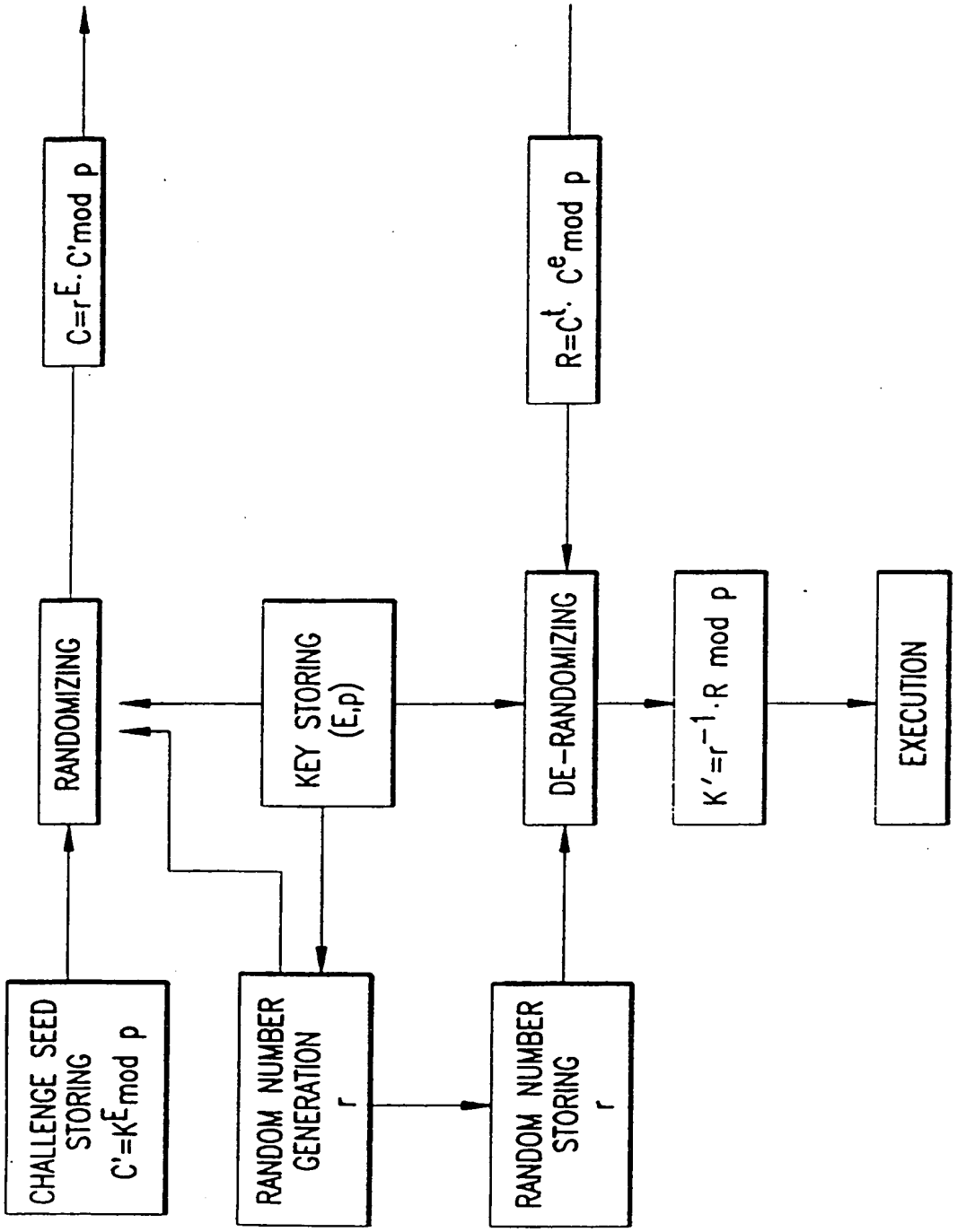

CHALLENGE SEED STORING C'=K^E mod p
RANDOMIZING
C=r^E. C' mod p
RANDOM NUMBER GENERATION r
KEY STORING (E,p)
RANDOM NUMBER STORING r
R=C^t. C^e mod p
DE-RANDOMIZING
K'=r^-1. R mod p
EXECUTION

FIG.21

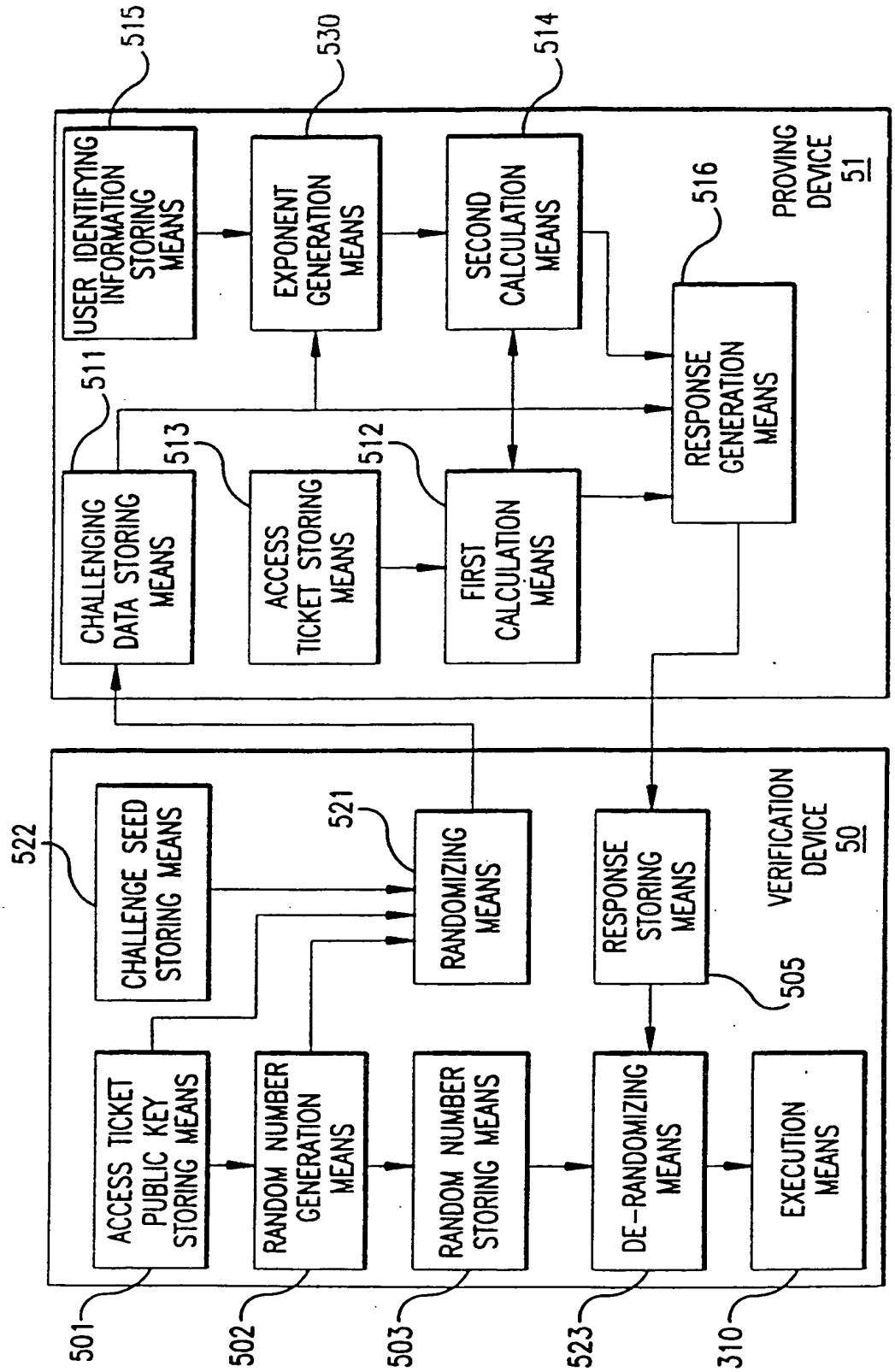

PROVING DEVICE 51
USER IDENTIFYING INFORMATION STORING MEANS
EXPONENT GENERATION MEANS
SECOND CALCULATION MEANS
RESPONSE GENERATION MEANS
CHALLENGING DATA STORING MEANS
ACCESS TICKET STORING MEANS
FIRST CALCULATION MEANS
515
530
514
516
511
513
512
VERIFICATION DEVICE 50
CHALLENGE SEED STORING MEANS
RANDOMIZING MEANS
RESPONSE STORING MEANS
ACCESS TICKET PUBLIC KEY STORING MEANS
RANDOM NUMBER GENERATION MEANS
RANDOM NUMBER STORING MEANS
DE-RANDOMIZING MEANS
EXECUTION MEANS
522
521
505
501
502
503
523
310

FIG.22

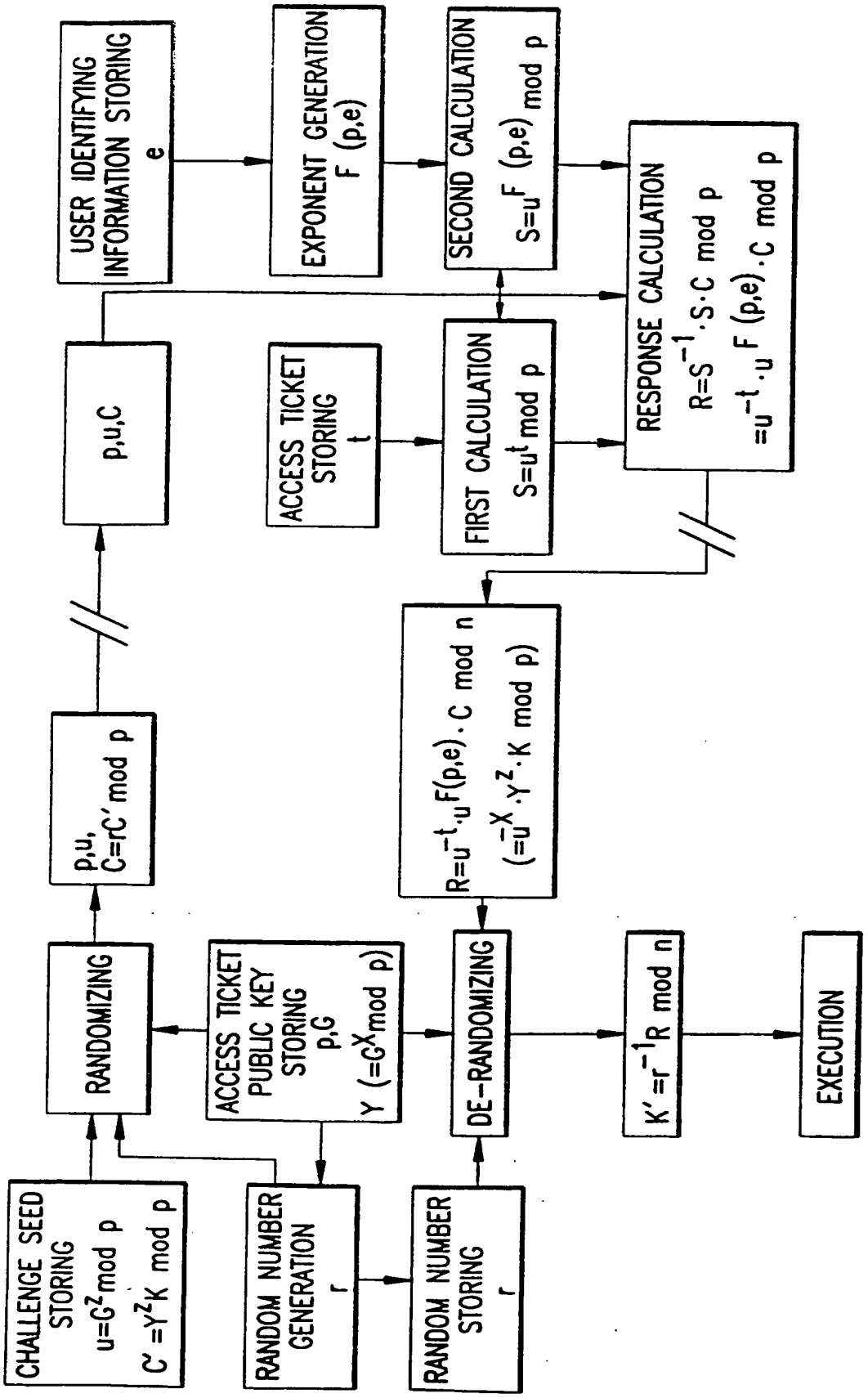

USER IDENTIFYING INFORMATION STORING
e
EXPONENT GENERATION
F (p,e)
SECOND CALCULATION
S=u^F (p,e) mod p
RESPONSE CALCULATION
R=S^-1 · S · C mod p
=u^-t · u^F (p,e) · C mod p
p,u,C
ACCESS TICKET STORING
t
FIRST CALCULATION
S=u^t mod p
R=u^-t · u^F(p,e) · C mod n
(=u^-X · Y^Z · K mod p)
p,u,
C=rC' mod p
RANDOMIZING
ACCESS TICKET PUBLIC KEY STORING
p,G
Y (=G^X mod p)
DE-RANDOMIZING
K'=r^-1 R mod n
EXECUTION
CHALLENGE SEED STORING
u=G^Z mod p
C'=Y^Z K mod p
RANDOM NUMBER GENERATION
r
RANDOM NUMBER STORING
r

FIG.23

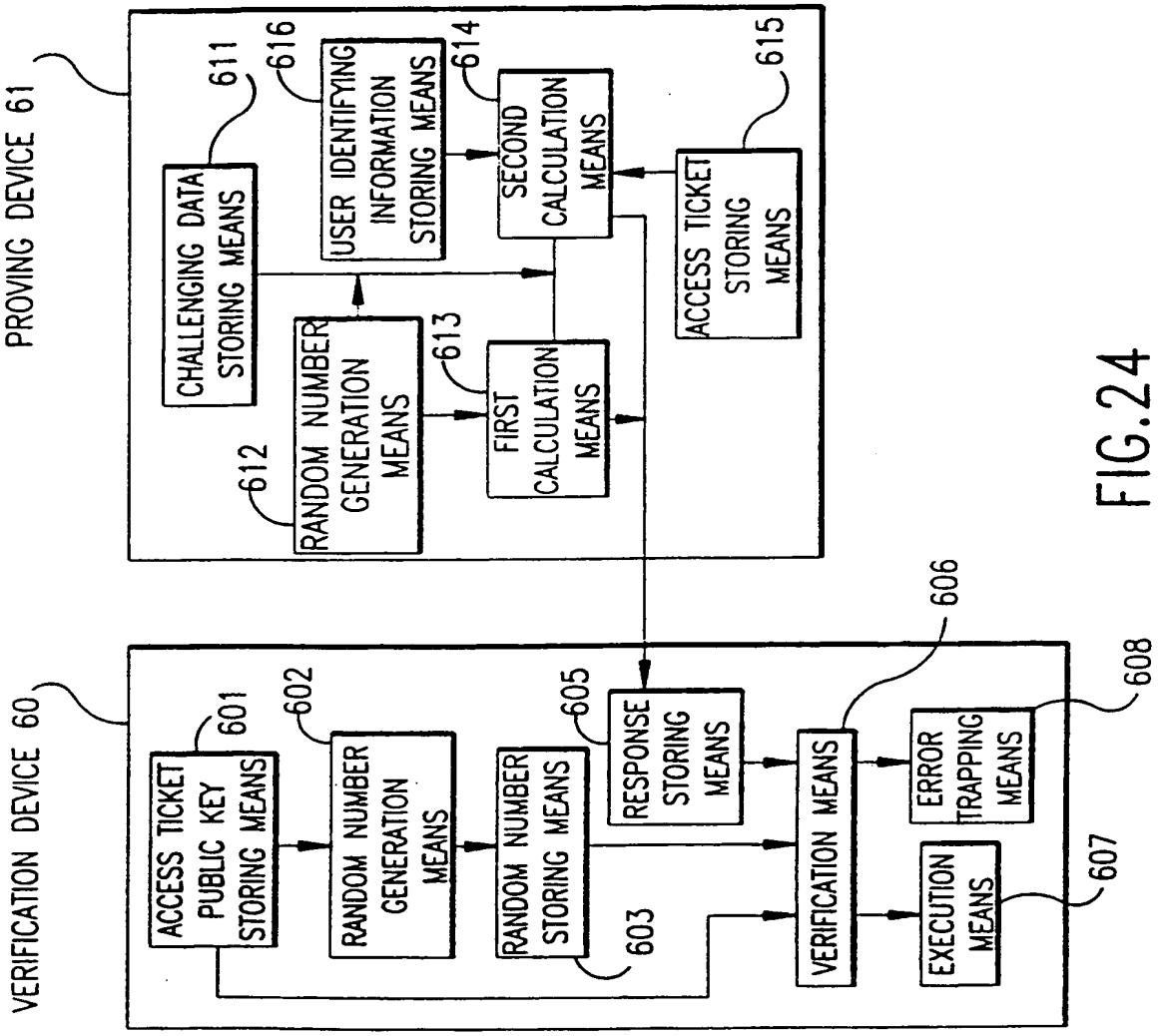

PROVING DEVICE 61
611
CHALLENGING DATA STORING MEANS
616
USER IDENTIFYING INFORMATION STORING MEANS
614
SECOND CALCULATION MEANS
615
ACCESS TICKET STORING MEANS
612
RANDOM NUMBER GENERATION MEANS
613
FIRST CALCULATION MEANS
VERIFICATION DEVICE 60
601
ACCESS TICKET PUBLIC KEY STORING MEANS
602
RANDOM NUMBER GENERATION MEANS
605
RANDOM NUMBER STORING MEANS
603
RESPONSE STORING MEANS
606
VERIFICATION MEANS
608
ERROR TRAPPING MEANS
607
EXECUTION MEANS

FIG.24

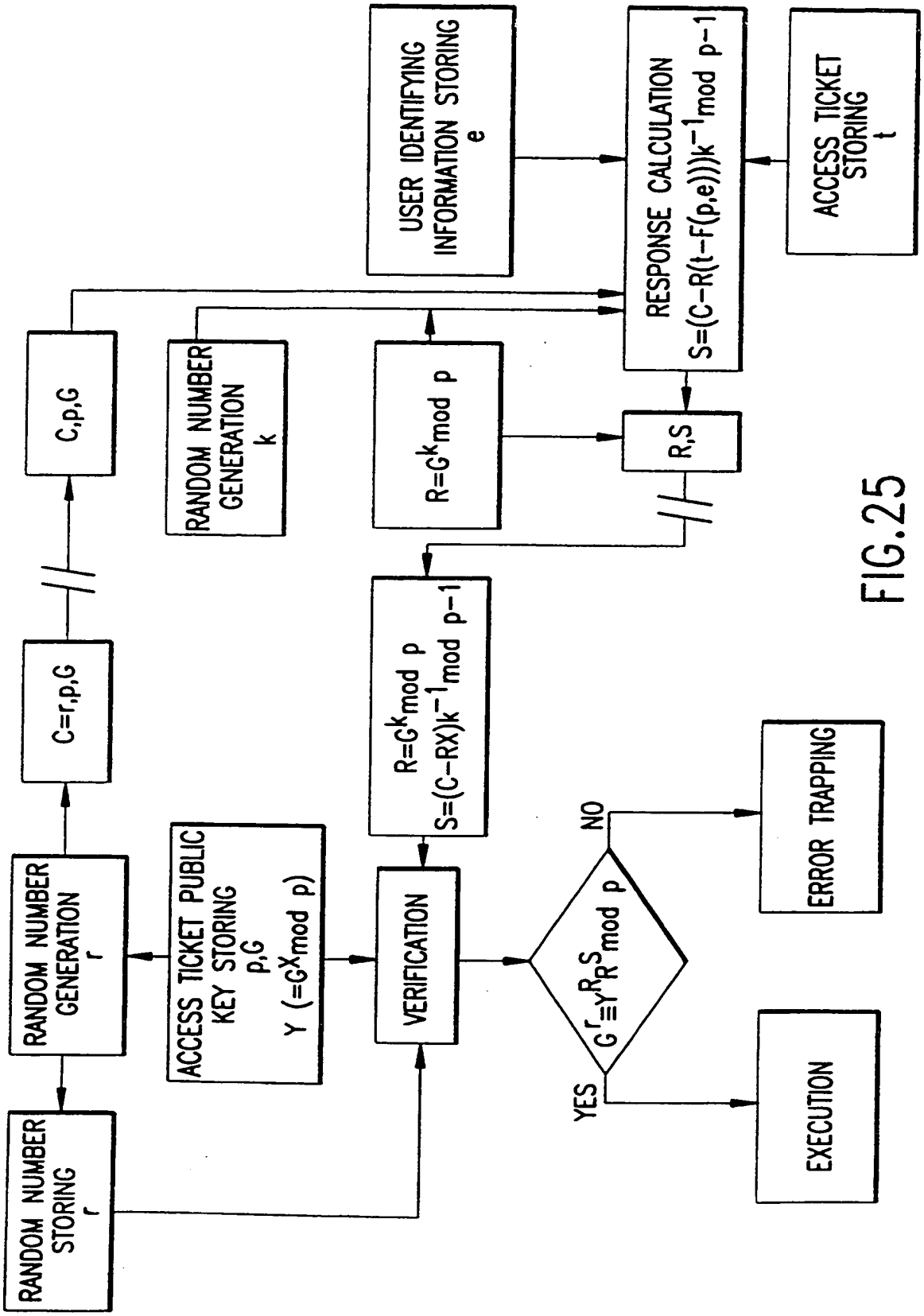

USER IDENTIFYING INFORMATION STORING e
RESPONSE CALCULATION S=(C−R(t−F(p,e)))k^−1 mod p−1
ACCESS TICKET STORING t
C,p,G
RANDOM NUMBER GENERATION k
R=G^k mod p
R,S
C=r,p,G
R=G^k mod p S=(C−RX)k^−1 mod p−1
RANDOM NUMBER GENERATION r
ACCESS TICKET PUBLIC KEY STORING p,G Y (=G^X mod p)
VERIFICATION
G^r≡Y^R R^S mod p
NO
ERROR TRAPPING
YES
EXECUTION
RANDOM NUMBER STORING r

FIG.25

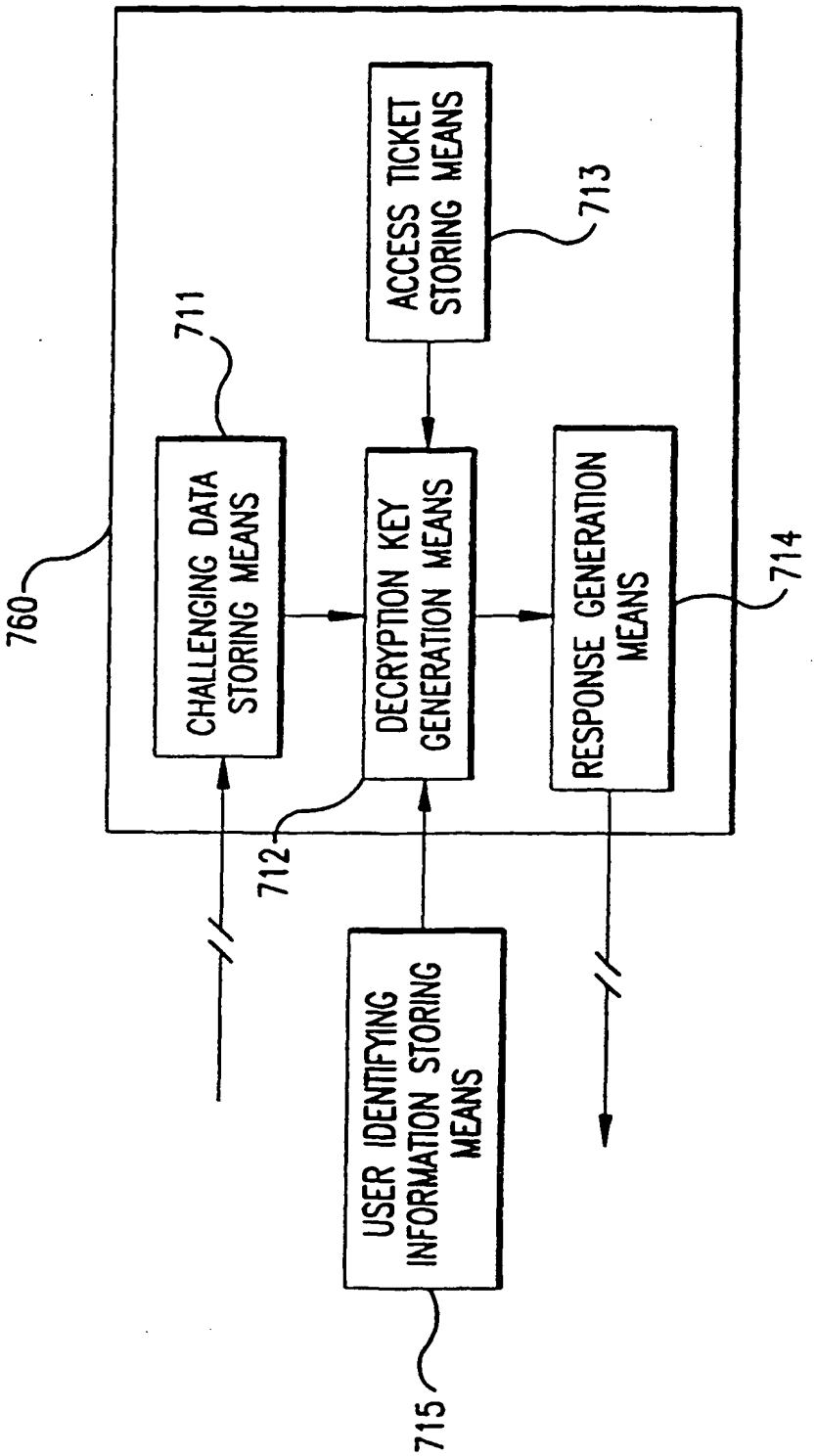

760
711
CHALLENGING DATA STORING MEANS
ACCESS TICKET STORING MEANS
713
DECRYPTION KEY GENERATION MEANS
RESPONSE GENERATION MEANS
714
712
USER IDENTIFYING INFORMATION STORING MEANS
715

FIG.26

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : G07F 7/10, H04L 9/00

A1

(11) International Publication Number: WO 89/11706

(43) International Publication Date: 30 November 1989 (30.11.89)

(21) International Application Number: PCT/US89/01944

(22) International Filing Date: 4 May 1989 (04.05.89)

(30) Priority data:

8811816.1	19 May 1988 (19.05.88)	GB
8906496.8	21 March 1989 (21.03.89)	GB
331,788	3 April 1989 (03.04.89)	US

(81) Designated States: AU, CH (European patent), DE (European patent), FR (European patent), GB (European patent), JP, NL (European patent).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(71) Applicant: NCR CORPORATION [US/US]; World Headquarters, Dayton, OH 45479 (US).

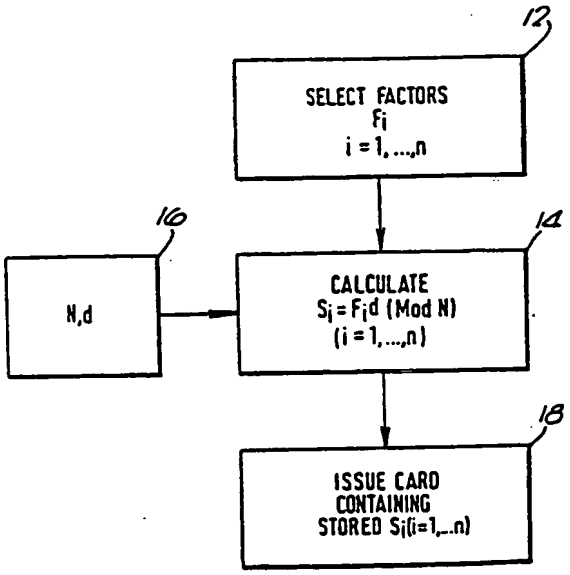
(72) Inventor: AUSTIN, Jeffrey, Reginald ; The White House, Tilford Road, Hindhead, Surrey GU26 6TD (GB).

(74) Agents: JEWETT, Stephen, F. et al.; Patent Division, NCR Corporation, World Headquarters, Dayton, OH 45479 (US).

(54) Title: METHOD AND DEVICE FOR AUTHENTICATION

(57) Abstract

An entity such as a smart card (30) includes microprocessor means (36), input/output means (44) and PROM storage means (42) which stores a set of transformations S_i (i = 1, ..., n) of a corresponding set of public factors F_i (i = 1, ..., n), where $S_i = F_i^d \pmod N$, d being the secret key counterpart of a public key e associated with the modulus N, which is the product of two primes. An authentication device (32) which stores the public factors F_i and the values of N and e, generates an n-bit random vector $V = v_i$ which is transmitted to the card (30) where a product Y of the values S_i selected according to the 1-bits of V is computed and transmitted to the authentication device (32) which computes $X_{act} = Y^e \pmod N$ and also computes X_{ref}, the product of the F_i selected according to the 1-bits of V. If X_{act} and X_{ref} are equal, then the card is authenticated to within a certain probability. An analogous method is disclosed for certifying messages to be transmitted. In further embodiments, a higher degree of security is achieved by arranging for the entity being authenticated, or the certifying entity, to select an additional secret factor or plurality of secret factors.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	ML	Mali
AU	Australia	FR	France	MR	Mauritania
BB	Barbados	GA	Gabon	MW	Malawi
BE	Belgium	GB	United Kingdom	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IT	Italy	RO	Romania
BJ	Benin	JP	Japan	SD	Sudan
BR	Brazil	KP	Democratic People's Republic of Korea	SE	Sweden
CF	Central African Republic			SN	Senegal
CG	Congo	KR	Republic of Korea	SU	Soviet Union
CH	Switzerland	LI	Liechtenstein	TD	Chad
CM	Cameroon	LK	Sri Lanka	TG	Togo
DE	Germany, Federal Republic of	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		
ES	Spain	MG	Madagascar		

METHOD AND DEVICE FOR AUTHENTICATION

This invention relates to the authentication of devices and messages.

It is a common requirement to verify the authenticity of data which may represent monetary value or may imply the authenticity of the entity generating that data.

To impede forgery, only a manufacturing source which produces entities should possess the means to produce authentication devices for the entities. This implies that the source must possess some secret. The difficulty in proving authenticity is in providing the means to the authenticator to achieve that proof. Many systems employ an algorithm driven by a secret key such that a data string passed through the algorithm results in a secret transformation of that data. The data so transformed is used as an authentication certificate or code which may be tested by an authenticator. One method of testing involves the authenticator in performing the same secret transformation of the data to yield an authentication certificate which is compared for equality with that provided by the source entity.

The problem with this technique is that the authenticator must duplicate the data manipulation by the source so as to compare the result for equality. This means that an authenticator can forge an authentication certificate and claim that it emanated from the source. Another problem is that the authenticator must also have knowledge of the key. This problem is particularly acute if several entities need to authenticate another entity, since each must possess the secret key. Disclosure of this key by one authenticator therefore compromises all authenticators and the source. Furthermore, the secret key must be securely distributed

to each potential authenticator prior to the event. This therefore limits the ability to authenticate to only those trusted entities which were anticipated to require the function.

Where it may be necessary for a large number of unpredictable entities to possess the ability to authenticate another entity, the use of secret key algorithms is somewhat impractical. Further, when it is desirable that the authenticator be completely denied the ability to forge an authentication certificate the duplicative equality test method cannot be employed.

Another known technique employs the art of public key cryptography wherein an asymmetrical algorithm is used. Public key cryptography is described in the article: Communications of the ACM, vol. 21, No. 2, February 1978, pages 120-126, R.L. Rivest et al. " A Method for Obtaining Digital Signatures and Public Key Cryptosystems". In this known technique, a data element or a change sensitive compression of a data string is enciphered using a secret key or procedure. Authenticity is proven by obtaining the original data element (or change sensitive compression) which is used as a reference value and then using a public key or procedure to decipher the data supplied by the source. Equality of the deciphered data with the reference data implies that the secret key or procedure was employed and thus that the data is authentic.

This technique permits any entity to know the public key or procedure with which to prove the authenticity of data emanating from an entity possessing the complementary secret key or procedure. Consequently, the key distribution problem is significantly eased as prior knowledge and secrecy are not required.

However, the publicly known procedure must not permit the secret key or procedure to be easily determined. Generally, the algorithms possessing this property require substantial computing power to perform the secret procedure. This usually renders them unsuitable for low cost devices where operational speed is a requirement. If multiple portable devices or the data emanating from them must be able to be tested for authenticity, then the secret key and algorithm must be contained in each device. In this case, disclosure of the secret key in one device will compromise all similar devices.

This technique is therefore not practical for low cost replicated devices.

European Patent Application No. 0 252 499 discloses a method for creating a unique card identifier in the form of a "smart card" which involves selecting a modulus which is a product of two primes, preparing a string of information unique to the card identifier, utilizing a pseudo-random function to transform such string and a plurality of selected indices to derive an associated plurality of values which are quadratic residues with respect to the modulus, computing the square roots of the reciprocals of the quadratic residues, and recording the information string, such square roots and the related indices in the card identifier. Such card is authenticated by transmitting the information string and the selected indices from the card to a verification device and generating in the verification device the quadratic residues utilizing the pseudo-random function, selecting in the card a random number, computing the squared value of the random number and transmitting such squared value from the card to the verification device, generating in the verification device a random vector which is sent to the card, computing in the card the product of the random number and a selection of the

stored square root values dependent on the random vector, transmitting the product to the verification device, squaring the transmitted product and multiplying such squared value by a selection of the computed quadratic residue values selected in accordance with the random vector, and checking that the result value is equal to the squared random number. This known method is complex and in particular involves the selection and utilization of quadratic residue values.

It is an object of the present invention to provide a relatively simple method and apparatus for the authentication of devices and messages.

Therefore, according to a first aspect of the present invention, there is provided a method of manufacturing an entity, including the steps of:

(a) selecting a modulus N which is a product of at least two prime numbers;

(b) selecting an integer e which is relatively prime to $\varphi(N)$, where $\varphi(N)$ is Euler's totient function of N; and

(c) determining an integer d such that $e \cdot d = 1 \pmod{\varphi(N)}$, characterized by the steps of:

(d) selecting a set of n public factors $F_1, \ldots, F_n$ $(0<F_i<N)$;

(e) calculating $S_i = F_i^d \pmod{N}$ for $i=1, \ldots, n$; and

(f) storing the n values S_i $(i=1, \ldots, n)$ and the value N in said entity.

According to a second aspect of the invention, there is provided a method of authenticating an entity according to the first aspect of the invention, characterized by the steps of:

(j) placing said entity in communication with an authentication device;

(k) generating in said authentication device an n-bit

binary string $V = v_i$ (i=1, ..., n)

(l) transmitting said binary string V to said entity;

(m) calculating, in said entity

$$Y = \prod_{v_i=1} S_i \pmod N;$$

(n) transmitting Y to said authentication device;

(o) calculating, in said authentication device

$$X_{ref} = \prod_{v_i=1} F_i \pmod N; \text{ and}$$

$$X_{act} = Y^e \pmod N; \text{ and}$$

(p) comparing X_{ref} and X_{act}.

According to a third aspect of the invention, there is provided a method of certifying a message M generated by or presented to an entity manufactured according to the first aspect of the invention, characterized by the steps of:

(q) computing a change-sensitive transformation H of said message M;

(r) generating an n-bit binary string $V = v_i$ (i=1, ..., n), using the computed value of H;

(s) computing

$$Y = \prod_{v_i=1} S_i \pmod N; \text{ and}$$

(t) appending Y as a message authentication code (MAC) certificate to said message M.

According to a fourth aspect of the invention, there is provided an entity including processing means, input/output means and memory means, characterized in that said memory means has stored therein a modulus N which is the product of at least two prime numbers and a set of n factors S_i (i=1, ..., n) where

$$S_i = F_i^{-d} \pmod N,$$

where d is the secret key counterpart of a public key e, associated with the modulus N, and F_i (i=1, ..., n) are n public factors, $0<F_i<N$, and wherein said processing

means is adapted to compute

$$Y = \prod_{v_i=1} S_i \pmod N$$

where $V = v_i$ is an n-bit binary string.

According to a fifth aspect of the invention, there is provided an authentication device for use with an entity according to the fourth aspect of the invention, including further processing means, further input/output means and further memory means, characterized in that said further memory means has stored therein said n public factors F_i (i=1, ..., n), said modulus N, and said public key e, and wherein said further processing means is adapted to compute

$$X_{ref} = \prod_{v_i=1} F_i \pmod N; \text{ and}$$

$$X_{act} = Y^e \pmod N$$

using the stored values of F_i, N and e, and to compare X_{ref} with X_{act}.

Embodiments of the present invention will now be described by way of example, with reference to the accompanying drawings, in which:-

Fig. 1 is a block diagram showing the procedure utilized by a card issuer in creating a smart card;

Fig. 2 is a block diagram of a card in operative association with a card acceptor device;

Fig. 3 is a block diagram of a message source unit;

Fig. 4 is a block diagram of a message authentication unit; and

Fig. 5 is a diagram showing the map of a memory utilized in an alternative embodiment of the invention.

Firstly, the theoretical basis underlying the invention will be explained, as an aid to understanding the invention. It is known that, if N is the product of (at least) two prime numbers P, Q, i.e., if

$$N = P.Q;$$

and if e is relatively prime to $\varphi(N)$, where

$$\varphi(N) = (P-1).(Q-1)$$

is Euler's totient function (the number of integers less than N which are relatively prime to N), then, in modulus N arithmetic, a value d can be determined (see for example, the aforementioned article by Rivest et al) which is the multiplicative inverse of e such that

$$e.d = 1 \pmod{\varphi(N)}.$$

The value d is commonly referred to as the secret key counterpart of the public key e.

Thus, if

$$X = Y^e \pmod N,$$

then

$$Y = X^d \pmod N$$

for all values of Y, $0<Y<N$.

Furthermore, if

$$X = F_1 . F_2 .... F_n \pmod N \qquad (1)$$

where F_i ($i = 1, \ldots, n$) are integer values, with

$$0<F_i<N$$

then

$$X^d = F_1^d . F_2^d .... F_n^d \pmod N$$

and

$$X^d \pmod N = \{F_1^d \pmod N . F_2^d \pmod N \ldots F_n^d \pmod N\} \pmod N$$

Let

$$S_i = F_i^d \pmod N;\ i=1, \ldots, n \qquad (2)$$

Then

$$X^d \pmod N = S_1 . S_2 \ldots S_n \pmod N$$

Let

$$Y = X^d \pmod N$$

Therefore

$$Y = S_1 \cdot S_2 \cdots S_n \pmod N \qquad (3)$$

Let V represent a binary string of n bits, $V = v_1 \cdots v_n$ such that each bit v_i of V is a flag indicating the inclusion of the corresponding $F_1, \ldots, F_n$ and $S_1, \ldots, S_n$ in the calculation of X and Y respectively, so that

$$X = \prod_{v_i=1} F_i \pmod N. \qquad (4)$$

From (3)

$$Y = \prod_{v_i=1} S_i \pmod N \qquad (5)$$

Therefore, provided that the N and d values employed in (1) and (2) satisfy the above requirements, then

$$X = \prod_{v_i=1} F_i \pmod N = \left\{\prod_{v_i=1} S_i \pmod N\right\}^e \pmod N$$

$$= Y^e \pmod N$$

for all values of F_i, $0<F_i<N$.

With the above in mind, a first embodiment of the invention will now be described, wherein multiple low cost devices, in the form of entities which will be referred to in the descriptions of the preferred embodiments as smart cards, are produced by a card issuer and distributed to individuals. The embodiment enables such issued cards to be expeditiously authenticated by verifying devices.

Referring first to Fig 1, a card issuer selects, as shown at box 12, a plurality of n public factors F_i ($i=1, \ldots, n$), where $0<F_i<N$, and such factors, together with the value of the modulus N and the value of e are made publicly available to authenticators, that is, organizations which may wish to authenticate smart cards issued by the smart card issuer. In a particular application a suitable value for n is 32, and the value of N is in the range $2^{512}<N<2^{513}$.

The card issuer computes the n values S_i, where

$S_i = F_i^d \pmod N \quad i=1, \ldots, n$

as shown at box 14, using provided values of N and d (box 16), where d is maintained secret. These values S_i are also maintained secret. The card issuer then issues cards which contain n values S_i (i=1, ..., n) stored in a secure manner, for instance in a secure PROM. It should be understood that by a "secure PROM" herein is meant a PROM the contents of which are protected from unauthorized read-out, for example, such protection may involve software protection and hardware protection in the form of shielding.

When it is desired to authenticate a smart card 30, Fig. 2, the card 30 is inserted into a card acceptor device 32, whereby a data communication path 34 is established between the smart card 30 and the card acceptor device 32.

The smart card 30 includes a microprocessor 36, a RAM 38, a program PROM 40 which stores the program controlling the operation of the card 30, a secure PROM 42 containing the n values S_i (i=1, ..., n) stored in respective storage locations 102-1 to 102-n and the value N stored in a storage location 104, and an input/output unit 44. Alternatively, since N is a public value, it could be stored in the RAM 38. The devices 36, 38, 40, 42 and 44 within the card are interconnected by a communications bus 46.

The card acceptor device 32 includes a microprocessor 50, a RAM 52, a program PROM 54 which stores the program controlling the operation of the acceptor device 32, a keyboard 56, a display 58, a printer 60, a random number generator 62, and an input/output unit 64. The RAM 52 includes storage locations 112-1 to 112-n storing the n public factors $F_1, \ldots, F_n$ and storage locations 114, 116 storing the values N and e, respectively. The various units located in the card acceptor device 32 are

interconnected by a communications bus 66.

When a card 30 inserted into the card acceptor device 32 is to be checked for authenticity, the random number generator 62 generates an n-bit random number V having n bits v_i (i=1, ..., n). In order to ensure that V contains at least two bits equal to binary 1, the microprocessor 50 is controlled, if necessary, to set the least significant bits of V progressively to binary 1 until at least two binary 1 bits are present in V. Thus, if the initial value of V is all zero bits, then the two least significant bits are set to binary 1. The value V is stored in the RAM 52.

The value V is then transmitted from the RAM 52 via the input/output unit 64 over the communication path 34 and the input/output unit 44 and is stored in the RAM 38 contained in the card 30. The microprocessor 36 checks that V contains at least two binary 1 bits, and if so, computes the value Y where

$$Y = \prod_{v_i=1} S_i \pmod N$$

using the values S_i stored in the PROM 42.

The value Y is then transmitted via the input/output unit 44, the transmission path 34 and the input/output unit 64 and is stored in the RAM 52. Using the values F_i (i=1, ..., n) V, and e, stored in the RAM 52, the microprocessor 50 then computes

$$X_{ref} = \prod_{v_i=1} F_i \pmod N$$

and

$$X_{act} = Y^e \pmod N,$$

and tests whether

$$X_{ref} = X_{act}.$$

Equality implies the authenticity of the X_{act} response

with probability of 1:N. The authenticity of the card 30 producing the response has a probability of $1:2^{n}-n$. By issuing repetitive random challenges in the form of random values of V, the probability that the card 30 is authentic increases exponentially by $1:(2^{n}-n)^{j}$ where j is the number of challenges issued.

It will be appreciated that the card 30 needs only to compute

$$Y = \prod_{v_i=1} S_i \pmod N$$

to respond to a challenge. Since this is at most n-1 multiplications using modulo N arithmetic, the work factor is significantly less than $Y = X_{ref}^{d} \pmod N$ for any large value of d. In this connection, it will be appreciated that since d is in effect the secret key associated with the card 30, and given that

$$e.d = 1 \pmod{\varphi(N)}$$

then d will be in the order of magnitude of 2N/3 for convenient values of e. Thus, in the described embodiment, authentication security comparable to that achievable with public key digital signature methods is achieved with significantly less computational effort. Furthermore, with no secret key used during the authentication process, it is possible to produce multiple cards 30 loaded with the $S_1, \ldots, S_n$ values which may be dynamically challenged by a verifying device to achieve similar confidence levels to those obtained with public key digital signature authentication methods.

It will be appreciated that the result of the authentication procedure can be indicated on the display 58 and/or recorded by the printer 60.

In a second embodiment of the invention, a data string forming a message M is authenticated by appending a certificate thereto. Such message M could, for example, be a data string representing a legal document, a

program file, or other information. Referring to Fig. 3, there is shown a message source unit 30A, which includes a message buffer 70 adapted to temporarily store a message M to be authenticated. The message source unit 30A further includes a microprocessor 36A, a RAM 38A, a program PROM 40A, a secure PROM 42A and an input/output unit 44A connected to a communications path 34A. The message source unit 30A also includes a communications bus 46A interconnecting devices 36A, 38A, 40A, 42A, 44A and 70 therein. It will be appreciated that the devices having the references with suffix A in Fig. 3 correspond to similarly referenced devices in the smart card 30 shown in Fig. 2, and in a practial implementation, the message source unit 30A could be a smart card. Furthermore, the secure PROM 42A stores the values S_1, S_2, ... S_n in locations 102A-1 to 102A-n, the value of the modulus N in storage location 104A and the value of e in storage location 106A. Clearly, the values of N and e, being public values, could alternatively be stored in the RAM 38a.

A message M stored in the message buffer 70 is authenticated by appending thereto a message authentication code (MAC) which is computed in the following manner.

Using the stored values of N and e, the microprocessor 36A first computes a change-sensitive transformation H of the message M. In the preferred embodiment, this is effected by computing:

$$H = M^e \pmod N$$

The value H is then converted to a binary value J, which is segmented into sub-fields of length n (with padding of an incomplete field with predetermined binary bits if necessary) and the individual sub-fields are added together modulo 2 (exclusive-or operation) such that the resultant binary string is used as $V = v_i$ $(i=1, \ldots, n)$ in the calculation of Y, where

$$Y = \prod_{v_i=1} S_i \pmod{N},$$

as described in the first embodiment.

This value of Y is then appended as a message authentication code (MAC) when the message M is transmitted from the message source unit 30A via the input/output unit 44A to a communication path 34A.

An authentication device 32A, Fig. 4, which is of generally similar construction to the card acceptor device 32 shown in Fig. 2 may be used to authenticate the transmitted message M. The authentication device 32A includes a message buffer 72, a RAM 52A, a program PROM 54A, a keyboard 56A, a display 58A, a printer 60A, an input/output unit 64A and an interconnecting communications bus 66A.

Stored in the RAM 52A, in locations 112A-1 to 112A-n, 114A and 116A, are the public factor values $F_1, \ldots, F_n$, together with the public key e and modulus N.

The message M, received over the communications path 34A is stored in the message buffer 72, together with the MAC, Y.

Using the received message M, the microprocessor 50A computes H and J to obtain V as in the message source unit 30A, and then computes

$$X_{ref} = \prod_{v_i=1} F_i \pmod{N}$$

utilizing the public factors F_i stored in the RAM 52A.

Using the received value Y stored in the message buffer 70, the microprocessor 50A then computes

$$X_{act} = Y^e \pmod{N}.$$

Finally, the values of X_{act} and X_{ref} are compared using the microprocessor 50A. Equality of X_{act} and X_{ref}

implies that the message source unit 30A possessed S_1, ..., S_n, and thus that the message M is authentic, within a probability of 1:N. It will be appreciated that this embodiment has the advantage that a low cost device (message source unit 30A) may readily certify data emanating from it with a probability of 1:N.

It should be understood that in the second embodiment, as in the first embodiment, in order to protect the S_i values from disclosure, it must be ensured that V contains at least two binary 1 bits, by progressively setting the least significant bits of V to binary 1 if necessary.

The second embodiment of the invention has the further advantage that several message source units 30A or the data emanating therefrom may be authenticated without the unit actually being present at the time of authentication. This ability is particularly useful for authenticating messages which may have been produced some time earlier by various message source units 30A, in the form of low cost devices such as smart cards. Multiple message source units may share the same F_1, ..., F_n values which would be standardized for the scheme, with individual integrity being ensured by various values of e and N.

However, it is preferred to standardize e and F_1, ..., F_n for all users of an authentication scheme within a group of users and for the operator of each message source unit to publish a specific value N to be used for his message source unit. Should an operator possess several such units, rather than specifying a unique value of N for each unit, integrity can be assured in a manner which will now be described with reference to the third embodiment of the invention.

According to a third embodiment of the invention, a

message M may be authenticated as originating from a unique message source unit among a set of such message source units sharing the same $F_1, \ldots, F_n$ and N and e values. This has the advantage that it is infeasible for one member of such a set to masquerade as another member of the set. For this purpose, the operator of the system allocates to each message source unit a public factor F_{ID} which is unique to that source unit. Furthermore, the operator of the system computes, for each such F_{ID} value, a corresponding S_{ID} value;

$$S_{ID} = F_{ID}^{d} \pmod{N},$$

where d is the system secret key, and stores S_{ID} in the secure memory of the relevant message source unit.

Referring to Fig. 5, there is shown a diagram of the secure PROM 42B included in the message source unit. The PROM 42B contains storage locations 102B-1 to 102B-n storing the n values $S_1, \ldots, S_n$, respectively, storage locations 104B and 106B storing the values N, e, respectively, and storage locations 108, 110, storing the values F_{ID}, S_{ID}, respectively.

In the third embodiment, it should be understood that the operation is generally similar to that described for the second embodiment, except that the calculation of the MAC, Y, is made according to the formula

$$Y = S_{ID} \cdot \prod_{v_i=1} S_i \pmod{N},$$

using the stored S_{ID} and S_i values. Correspondingly, the calculation of X_{ref} in the message authentication unit is made according to the formula

$$X_{ref} = F_{ID} \cdot \prod_{v_i=1} F_i \pmod{N},$$

using the stored F_i values, with the F_{ID} value being included in the certified message transmitted from the message source unit to the message authentication unit for use in the computation of X_{ref}.

It will be appreciated that in the third embodiment,

with S_{ID} included in the computation of Y, the requirement that V contains at least two binary 1 bits is reduced to the requirement that V should be non-zero.

The embodiments described hereinabove may be used for any application where it is desired to authenticate entities or the data emanating from them. An important application, however, is to an intelligent financial transaction token or smart card used in Electronic Funds Transfer at the Point of Service (EFTPOS). For several reasons of cost and security it is perceived that the so called "smart card" provides a highly effective technology for EFTPOS.

A fundamental reason for using smart card technology is to enable a transaction to be completed fully off-line from the card issuer's authorization system with a minimum of risk to the various parties affected.

From a risk analysis point of view, the following areas must be considered

(a) Is the card holder legitimate?

(b) Is the card authentic?

(c) Is the implied value loaded into or dispensed by the card authentic?

(d) Is the transaction claim made by the card acceptor authentic?

Card holder authenticity is generally effected by employing a Personal Identification Number (PIN) which is verified by or with the smart card prior to sensitive operations being initiated. Such PIN may be entered via a keyboard such as the keyboard 56, Fig. 2, or by a keyboard (not shown) integral with the card.

It is commonly perceived that card authenticity needs to be established prior to transferring value to prevent bogus funds being loaded into or dispensed by the card. However, this requirement in essence occurs with many

implementations because it is not possible to authenticate at the point of service the value data exchanged.

Therefore, considering the dispersal of value from a card, provided that the card could itself produce an authentication certificate for the data emanating from it such that the certificate could be tested by any other entity, then card authentication is unnecessary. This has significant consequence for remote card authentication or home banking applications, as the need for a trusted card authentication device at the point of card acceptance is eliminated. This possibility also enables any intermediate entity handling the value message between the card and the entity guaranteeing the funds to test the authenticity of the data in order to undertake settlement actions. In this sense, the potential exists for true electronic currency.

Considering the loading of value, if it can be shown that data emanating from a card is authentic, it must be assumed that only an authentic card could perform the certificate calculation corectly. Therefore, if only an authentic card can correctly dispense funds, then the requirement of preventing the loading of bogus value can be readily met by designing authentic cards such that they will reject an attempted loading of bogus value themselves.

Since the card contains the ability to generate certificates, it could therefore check a certificate as well. This could be done in a fourth embodiment of the invention by calculating a certificate for value load data presented to the card in the same manner as done by the card itself and appending that certificate to the value load data. The card could replicate that operation and compare the result with the presented certificate. The presumption is that only the entity guaranteeing dispensed value could correctly load value so

that it is assumed that this entity knows the secret certificate calculation method.

However, this technique would require the entity generating the load value certificate to have available a record of each card's secrets (given the potential size of card networks, the possibility that several value generators may wish to load value, and the highly desirable need to uniquely authenticate each card) this requirement could become impractical.

The primary advantage of the embodiments described hereinabove is that any entity may easily test the authenticity of data emanating from another entity. If it was considered that the source of the value load data was a similar entity to the load accepting entity, then any other entity including the destination card itself could similarly easily test the load data for authenticity prior to acceptance.

Thus, the need to authenticate a card or, conversely, the need for the card to authenticate the load device is eliminated if the techniques of public message authentication as described in the third embodiment are employed.

Thus, the fourth embodiment of the invention provides a means and method for eliminating the need for trusted terminal devices, which may have the capability of adding information or value to the entities in the set, by delivering such information with an authentication certificate such that the member entity can authenticate that information as emanating from the identified source prior to its acceptance. In the fourth embodiment the member entity (smart card) possesses both the ability to generate its own certificates and also test certificates from other entities by employing in the first case the techniques of the third embodiment to generate certi-

ficates and in the second case the complementary techniques of the third embodiment to test certificates.

In this fourth embodiment, the card may additionally contain stored therein the F_i, N and e values appropriate for each value load generator which is authorized by the card issuer to perform the value load function. For convenience, all generators should employ the same public factors F_i and public key e, with individual integrity being obtained by the use of different N values.

Although in the preferred embodiments, the calculations within the card 30, and acceptor device 32, message source unit 30A and message authentication unit 32A have been described as being effected by microprocessors 36, 50, 36A, 50A, it should be understood that in a modification, each microprocessor may be associated with a respective dedicated calculation unit which performs the function

$$f(P) = P.M \pmod{N}.$$

Such dedicated circuitry may use shift register and serial adder/subtractor elements such that a value M is multiplied by a value P while simultaneously the value N is subtracted, if necessary, to yield within a single computation cycle the desired product value P.M (mod N). By this means, the function

$$Y = \overline{\prod_{v_i=1} S_i} \pmod{N}$$

may be computed with the values S_i being progressively presented as indicated by the values of the bits v_i of V.

The embodiments described above provide a high degree of security both for the authentication of entities and for the certification of messages. However, it should be understood that, depending on system implementation, a sophisticated attacker could compromise a system employing such authentication and/or certification techniques, as will now be explained. Thus, since the factors F_i and S_i are selected for multiplication according to the value of V, it follows that, if the system design permitted an appropriately manipulated authentication device to generate any desired values of V, for example, if the values

$$V_a = 3 \text{ (decimal)} = 011 \text{ (binary)}$$

and $V_b = 7$ (decimal) = 111 (binary)
could be freely chosen, then corresponding Y values

$$Y_a = S_1.S_2 \pmod N$$

and $Y_b = S_1.S_2.S_3 \pmod N$
would be produced.

Since

$$S_3 = Y_b/Y_a = (S_1.S_2.S_3)/(S_1.S_2) \pmod N,$$

S_3 is disclosed. Similarly, any desired S_i can be ascertained, provided that division operations can be effected. Due to the modulus N operation on Y_a and Y_b, simple division will not necessarily yield a correct value. However, since N is a composite of large prime numbers (usually two), then most numbers in the range 1 to N-1 will have a modulo N reciprocal, i.e. given Y, there is, generally, a value Y^{-1}, such that

$$Y.Y^{-1} = 1 \pmod N$$

Known mathematical techniques can be utilized to find such reciprocal value Y^{-1}.
Hence, $S_3 = Y_b.Y_a^{-1} \pmod N$
can be determined, and, by similar techniques, the remaining S_i can also generally be ascertained. Having ascertained the S_i values, the sophisticated attacker,

using suitable hardware could fraudulently effect authentication and certification procedures.

To avoid such an attack, it should be made infeasible to select V values which yield a set of Y values which can be manipulated to yield single factors S_i.

In a fifth embodiment of the invention, this problem is alleviated by including an additional public parity factor F_p and associated secret factor S_p in the system, where

$$S_p = F_p^d \pmod{N},$$

and arranging that all Y values are the product of an even number of factors, utilizing S_p if necessary, thus preventing the ascertainment of any single factor. For example, with this arrangement,

for V = 1 (decimal), $Y = S_1 \cdot S_p \pmod{N}$

for V = 2 (decimal), $Y = S_2 \cdot S_p \pmod{N}$

for V = 3 (decimal), $Y = S_1 \cdot S_2 \pmod{N}$, etc.

Thus, in the arrangement described with reference to Fig. 1, a card issuer selects an additional public factor F_p, calculate S_p and store S_p in the cards to be issued. Similarly, in the message certification system described with reference to Figs. 3 and 4, the additional secret parity factor S_p is stored in the PROM 42A and the corresponding public parity factor F_p stored in the RAM 52A. Again, with the unique identification arrangement described with reference to Fig. 5, the secret parity factor S_p is stored in the secure PROM 42B, in addition to the S_{ID} value, and with this arrangement, there is the further advantage that V can be in the full range of 0 to 2^n-1. This is desirable for message certification since it eliminates any need to adjust the message hash result. Thus, with this arrangement,

for V = 0 (decimal), $Y = S_{ID}.S_p \pmod N$

for V = 1 (decimal), $Y = S_{ID}.S_1 \pmod N$

for V = 2 (decimal), $Y = S_{ID}.S_2 \pmod N$

for V = 3 (decimal), $Y = S_{ID}.S_1.S_2.S_p \pmod N$, etc.

Although it could be argued that if the fifth embodiment is utilized, an attacker could selectively extract all factor pairs,

e.g. $S_1.S_2 = V_3.V_0^{-1}$,

and use these pairs to produce bogus certificates in a message certification scheme, such an attack may be infeasible due to the number of pairs needed to be obtained and fraudulently used in systems where n has a suitably large value.

Another way to prevent selective extraction of S_i values by an attacker is to ensure that any Y value is not consistently related to any other Y value. This can be achieved by including a variable component in the Y calculation which cannot be controlled or predicted by an attacker. Such variable component should be chosen from a large enough set of possible component values to make the reoccurrence of any specific value statistically improbable. That is, the number of Y values needing to be obtained to ensure that the same variable component is included in the calculation, should be infeasibly large for an attacker.

Firstly, it will be appreciated that the Y values are in fact a base set of 2^n values pseudo-randomly distributed within the set bounded by 1 and N-1. Secondly, it will be appreciated that the numerical separation of these Y values is in fact precisely determined. Application of an offset value which was applied to all Y values in the base set would in effect produce another set of

precisely separated Y values within the set 1, N-1. Thus, provided that the number of Y sets which could be produced by offset was large enough to be statistically unique, then mathematical extraction of the factors making up a certain Y value would be infeasible, unless the set offset value was known, since the number of valid Y values within the set 1, N-1 would be increased from 2^n to 2^n times the number of Y sets.

In the extreme case, consider that the number of Y sets was N-1 then the number of valid Y values would be $2^n.(N-1)$. This would raise the probability that an entity producing a Y value was authentic, or that a message from the entity was authentic, from 2^n to $2^n.(N-1)$. For typical N values $2^{512} < N < 2^{513}$ then the order of probability of authenticity would be $2n.2^{512}$. This is not true in practice since the total of Y values available is N-1, limiting the probability to 1:(N-1). Clearly since this order of probability far exceeds any reasonable requirement, the number of Y sets could be substantially reduced. If s equals the number of binary bits available to denote the set number then the number of sets would be 2^s giving an authenticity probability of $2^n.2^s$ or 2^{n+s}. Note that in principle n and s could be varied in size to obtain the order of probable authenticity protection desired in the system. However, since the 2^n component may be selectable via V by an attacker the 2^s component should be large enough to make such an attack infeasible. Also, note that n determines the range of V and should be large enough to preclude undetected manipulation of message contents when V results from a hash function of a message.

In such a system it is necessary to communicate to the authenticator the Y set employed for a particular Y calculation by the certifying entity. If this was directly disclosed as an offset value, then the

aforementioned attacks could still be executed since reversing the offset process would yield the original base set of Y values and thus by extraction, the base set of S_i values. Consequently, the offset value or set identifier should be provided in a manner usable by the authenticator for Y testing but not for Y factoring.

For example, it is possible to include in the authentication protocol a value F_{set} which is passed to the authenticator for each Y calculation. F_{set} is produced by the certifier selecting a set number S_{set} and computing

$$F_{set} = S_{set}^{e} \pmod{N}$$

Note that S_{set} cannot be determined from F_{set} without knowledge of d. Thus, for entity authentication, the entity:

(i) Selects an S_{set}

(ii) Computes $F_{set} = S_{set}^{e} \pmod{N}$

(iii) Communicates F_{set} to the authentication device, which

(iv) Selects a V value and communicates this value to the entity, which computes

(v) $Y = S_{set} \cdot \prod_{V_i=1} S_i \pmod{N}$ which it communicates to the authentication device, which tests Y by

(vi) $X_{ref} = F_{set} \cdot \prod_{V_i=1} F_i \pmod{N}$

$= X_{act} = Y^{e} \pmod{N}$.

Note that, since F_{set} is a pseudo-random distribution within the set 1, N-1 from which it is not feasible to determine S_{set}, then it is not necessary to choose S_{set} randomly. The protection from analytical attacks can be obtained merely by ensuring that S_{set} does not predictably repeat within an attack session. One such method to achieve this is to run an incremental count of Y

calculations and to use this count value to update S_{set}. This method has the further advantage of providing to the entity originator a method of cryptographically checking for lost or duplicated messages delivered to him from the source entity.

Thus, in a sixth embodiment of the invention, for message certification,

$$Y = S_{ID} \cdot S_{set} \cdot \prod_{V_i=1} S_i \cdot S_p \pmod{N}$$

where S_{set} = a function of the counter value

$S_{ID} = F_{ID}^{d} \pmod{N}$

$S_i = F_i^{d} \pmod{N}$

$S_p = F_p^{d} \pmod{N}$ optionally included if V has even parity,

and the certificate Y is calculated across a message including F_{ID}, F_{set} therein, where $F_{set} = S_{set}^{e} \pmod{N}$.

To generate the S_{set} counter values a hardware counter could be provided in a smart card or entity to be authenticated, such as the card 30, Fig. 2, or in a message source unit such as the message source unit 30A, Fig. 3. Alternatively, the microprocessor 36 or 36A therein could be programed to provide a counting operation using storage locations in the RAM memories 38 or 38A. An analogous arrangement could be utilized when a unique identifier factor S_{ID} and associated F_{ID} are employed as described hereinabove with reference to the third embodiment of the invention.

In the just mentioned system the protocol is enlarged by the inclusion of F_{set}. This is unimportant for interactive entity authentication by locally communicating devices but may be an unacceptable overhead for message certification.

A further method of pseudo-randomly varying the base set of Y values which does not add significantly to the protocol is to utilize precalculated offset values the selection of which is advised to the authentication device.

In a seventh embodiment of the invention, V, which is made up of n bits, is split into two parts, V_s and V_a, where V_s is chosen by the certifier, and V_a as before is chosen in the authentication device (or determined by the message content). The number of bits in each of V_s and V_a is predetermined. For example, where n=32, each of V_s and V_a could have 16 bits. The bits of V_s are used to select the S_{set} offset value with the bits of V_a being used to select the S_a values. Note also that the S_{set} offset values can be combined to yield 2^{ns} offset values, where ns is the number of base offset values available.

Thus, in the seventh embodiment,

$$Y = \prod_{V_{si}=1} S_{si} \cdot \prod_{V_{ai}=1} S_{ai} \pmod N;$$

$$X_{ref} = \prod_{V_{si}=1} F_{si} \cdot \prod_{V_{ai}=1} F_{ai} \pmod N; \text{ and}$$

$X_{act} = Y^e \pmod N$, as before.

The values $S_{si} = F_{si}^d \pmod N$ are stored by the certifier (smart card or message source unit) and used in a similar manner to the S_{ai} values, but selected by the certifier pseudo-randomly.

The values F_{si} are made publicly available in the same manner as the F_{ai} values.

In this embodiment, V_s rather than F_{set} would be

included (and hashed for V_a) in the certified message.

Thus, for message certification where the unique identifier factors

S_{ID} and F_{ID} are utilized,

$M = V_S, F_{ID}$, Message.

As in the second embodiment, a change-sensitive transformation H of the aggregate message M is formed, and the value of V_a derived therefrom. The following calculations are then effected:

$$Y = S_{ID} \cdot \prod_{V_{si}=1} S_{si} \cdot \prod_{V_{ai}=1} S_{ai} \pmod N; \text{ and}$$

$$X_{ref} = F_{ID} \cdot \overline{\prod_{V_{si}=1}} F_s \cdot \overline{\prod_{V_{ai}=1}} F_{ai} \pmod N.$$

It can be seen from the above that the authenticity of a particular Y value is as before 1:N. The authenticity of the entity producing the Y value (entity forgery) is determined by the number of bits in V_S and V_a and is therefore $1:2^{ns+na}$.

CLAIMS

1. A method of manufacturing an entity (30, 30A), including the steps of:

(a) selecting a modulus N which is a product of at least two prime numbers;

(b) selecting an integer e which is relatively prime to $\varphi(N)$, where $\varphi(N)$ is Euler's totient function of N; and

(c) determining an integer d such that $e.d = 1 \pmod{\varphi(N)}$, characterized by the steps of:

(d) selecting a set of n public factors $F_1, \ldots, F_n$ $(0<F_i<N)$;

(e) calculating $S_i = F_i^d \pmod{N}$ for i=1, ..., n; and

(f) storing the n values S_i (i=1, ..., n) and the value N in said entity.

2. A method according to claim 1, characterized in that said n values S_i are stored in a programmable read-only memory (PROM) (42, 42A, 42B) included in said entity (30, 30A).

3. A method according to claim 2, characterized in that said entity (30, 30A) includes processing means (36, 36A) and input/output means (44, 44A).

4. A method according to claim 1, characterized by the steps of:

(g) assigning a public factor F_{ID} unique to said entity;

(h) computing $S_{ID} = F_{ID}^d \pmod{N}$; and

(i) storing the value S_{ID} in said entity.

5. A method of authenticating an entity (30, 30A) according to any one of claims 1 to 4, characterized by the steps of:

(j) placing said entity (30, 30A) in communication with an authentication device (32, 32A);

(k) generating in said authentication device (32, 32A) an n-bit binary string $V = v_i$ (i=1, ..., n)

(l) transmitting said binary string V to said entity (30, 30A);

(m) calculating, in said entity (30, 30A)

$$Y = \prod_{v_i=1} S_i \pmod N;$$

(n) transmitting Y to said authentication device (32, 32A);

(o) calculating, in said authentication device (32, 32A)

$$X_{ref} = \prod_{v_i=1} F_i \pmod N; \text{ and}$$

$$X_{act} = Y^e \pmod N; \text{ and}$$

(p) comparing X_{ref} and X_{act}.

6. A method according to claim 5, characterized in that said authentication device (32, 32A) includes storage means (52, 52A) adapted to store said public factors F_1, ..., F_n, and the values of N and e.

7. A method according to claim 6, characterized by the step of repeating said steps (k) to (p) a plurality of times, using random values of V.

8. A method of certifying a message M generated by or presented to an entity (30, 30A) manufactured according to any one of claims 1 to 4 characterized by the steps of:

(q) computing a change-sensitve transformation H of said message M;

(r) generating an n-bit binary string $V = v_i$ (i=1, ..., n), using the computed value of H;

(s) computing

$$Y = \prod_{v_i=1} S_i \pmod N; \text{ and}$$

(t) appending Y as a message authentication code (MAC) certificate to said message M.

9. A method according to claim 8, characterized in that said step of (q) computing said change-sensitive transformation H is effected by computing

$$H = M^e \pmod N.$$

10. A method according to claim 8 or 9, characterized in that said step of (r) generating an n-bit binary string V is effected by the steps of:

(u) converting H to a binary value J;

(v) segmenting J into sub-fields of length n; and

(w) adding together the individual sub-fields modulo 2 to form said n-bit binary string V.

11. A method according to any one of claims 5 to 10, characterized in that, in said step (m) and said step (s) the value of Y is calculated according to the formula

$$Y = S_{set} \cdot \prod_{V_i=1} S_i \pmod N,$$

where S_{set} is selected in said entity (30,30A);

by the steps of

(x) computing in said entity (30,30A) $F_{set} = S_{set}^e \pmod N$, and

(y) transmitting F_{set} to said authentication device (32,32A);

and in that in said step (o), the value of X_{ref} is calculated according to the formula

$$X_{ref} = F_{set} \cdot \prod_{V_i=1} F_i \pmod N.$$

12. A method according to claim 11, characterized in that S_{set} is selected in accordance with a count value which is incremented for each Y caluculation.

13. A method according to claim 12, characterized in that S_{set} is determined by computing,

in said entity (30,30A), a product including a selection of a set S_{si} of said factors S_i, said selection being in accordance with a binary string $V_s = v_{si}$ generated in said entity (30,30A), whereby the value of Y is calculated according to the formula.

$$Y = \prod_{v_{si}=1} S_{si} \cdot \prod_{v_{ai}=1} S_{ai} \pmod N,$$

wherein the v_{ai} values corresponding to the bits of said n-bit binary string generated in said authentication device (32,32A);

by the step of:

(z) transmitting V_s to said authentication device (31,32A), and in that the value of X_{ref} is calculated in said authentication device (32,32A) according to the formula

$$X_{ref} = \prod_{v_{si}=1} F_{si} \cdot \prod_{v_{ai}=1} F_{ai} \pmod N.$$

14. A method according to any one of claims 5 to 13, characterized in that, in said step (m) and said step (s), the value of Y is calculated utilizing selectively an additional predetermined factor S_p, such that the total number of factors included in the calculation of Y is even, and in that, in said step (o), the value of X_{ref} is correspondingly calculated, utilizing selectively an additional factor F_p, where $S_p = F_p^d$.

15. An entity (30,30A), including processing means (36,36A), input/output means (44,44A) and memory means (42,42A,42B), characterized in that said memory means (42,42A,42B) has stored therein a modulus N which is the product of at least two prime numbers and a set of n factors S_i (i=1, ..., n) where

$$S_i = F_i^d \pmod N,$$

where d is the secret key counterpart of a public key e, associated with the modulus N, and F_i (i=1, ..., n) are

n public factors, $0<F_i<N$, and in that said processing means (36,36A) is adapted to compute

$$Y = \prod_{V_i=1} S_i \pmod N$$

where $V = V_i$ is an n-bit binary string.

16. An entity according to claim 15, characterized in that said memory means (42A,42B) is further adapted to store the value of said public key e and in that said processing means is further adapted to compute

$$H = M^e \pmod N$$

where M is a message to be transmitted by said entity (30,30A), to convert H to a binary n-bit vector V, and to compute

$$Y = \prod_{v_i=1} S_i \pmod N.$$

using the bits v_i of the computed vector V, and in that said input/output means (44,44A) is adapted to transmit Y as a message authentication code (MAC) associated with said message.

17. An entity according to claim 15 or 16, characterized in that said memory means (42B) has stored therein a public factor F_{ID} unique to said entity, and a value S_{ID}, where

$$S_{ID} = F_{ID}^{d} \pmod N.$$

18. An entity according to any one of claims 15 to 17, characterized in that the value of Y includes an additional factor S_{set} which is dependent on a count value which is incremented for each Y calculation.

19. An entity according to any one of claims 15 to 18, characterized in that said memory means (42,42A,42B) has stored therein an additional parity factor S_p, and in that said processing means (36,36A) is

adapted to compute the value of Y by selectively including said additional parity factor S_p in the expression for Y, such that the total members of factors included in the calculation of Y is even.

20. An authentication device (32, 32A) for use with an entity (30, 30A) according to any one of claims 15 to 19, including further processing means (50, 50A), further input/output means (64, 64A) and further memory means (52, 52A), characterized in that said further memory means (52, 52A) has stored therein said n public factors F_i (i=1, ..., n), said modulus N, and said public key e, and wherein said further processing means (50, 50A) is adapted to compute

$$X_{ref} = \overline{\prod_{v_i=1} F_i} \pmod N; \text{ and}$$

$$X_{act} = Y^e \pmod N$$

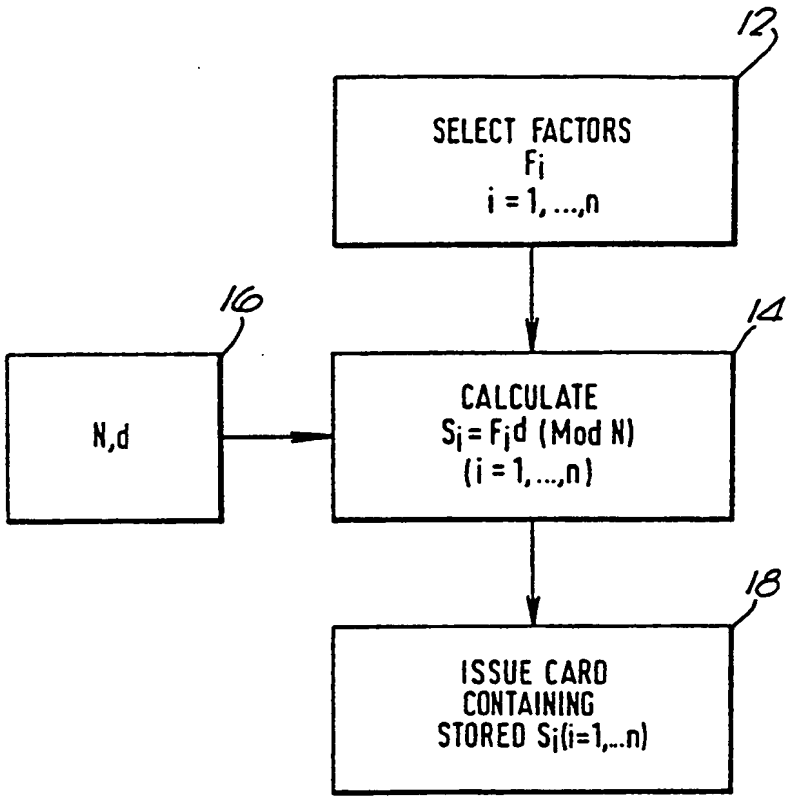
using the stored values of F_i, N and e, and to compare X_{ref} with X_{act}.

21. An authentication device according to claim 20 for use with an entity according to claim 17, characterized in that said further processing means is further adapted to compute

$$X_{ref} = F_{ID} \cdot \overline{\prod_{v_i=1} F_i} \pmod N$$

22. An entity according to any one of claims 15 to 19, characterized in that said entity incorporates an authentication device according to claim 20 or claim 21.

FIG. 1


12
SELECT FACTORS
Fi
i = 1, ...,n
16
N,d
14
CALCULATE
Si = Fid (Mod N)
(i = 1, ...,n)
18
ISSUE CARD
CONTAINING
STORED Si(i=1,...n)

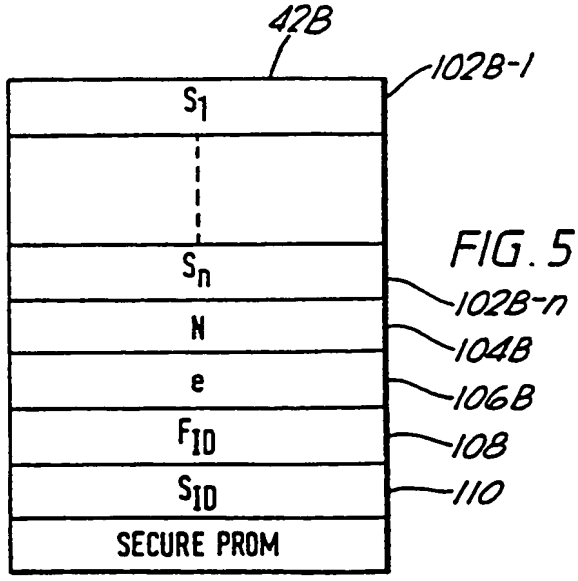

42B
102B-1
S1
Sn
102B-n
N
104B
e
106B
FID
108
SID
110
SECURE PROM

FIG. 5

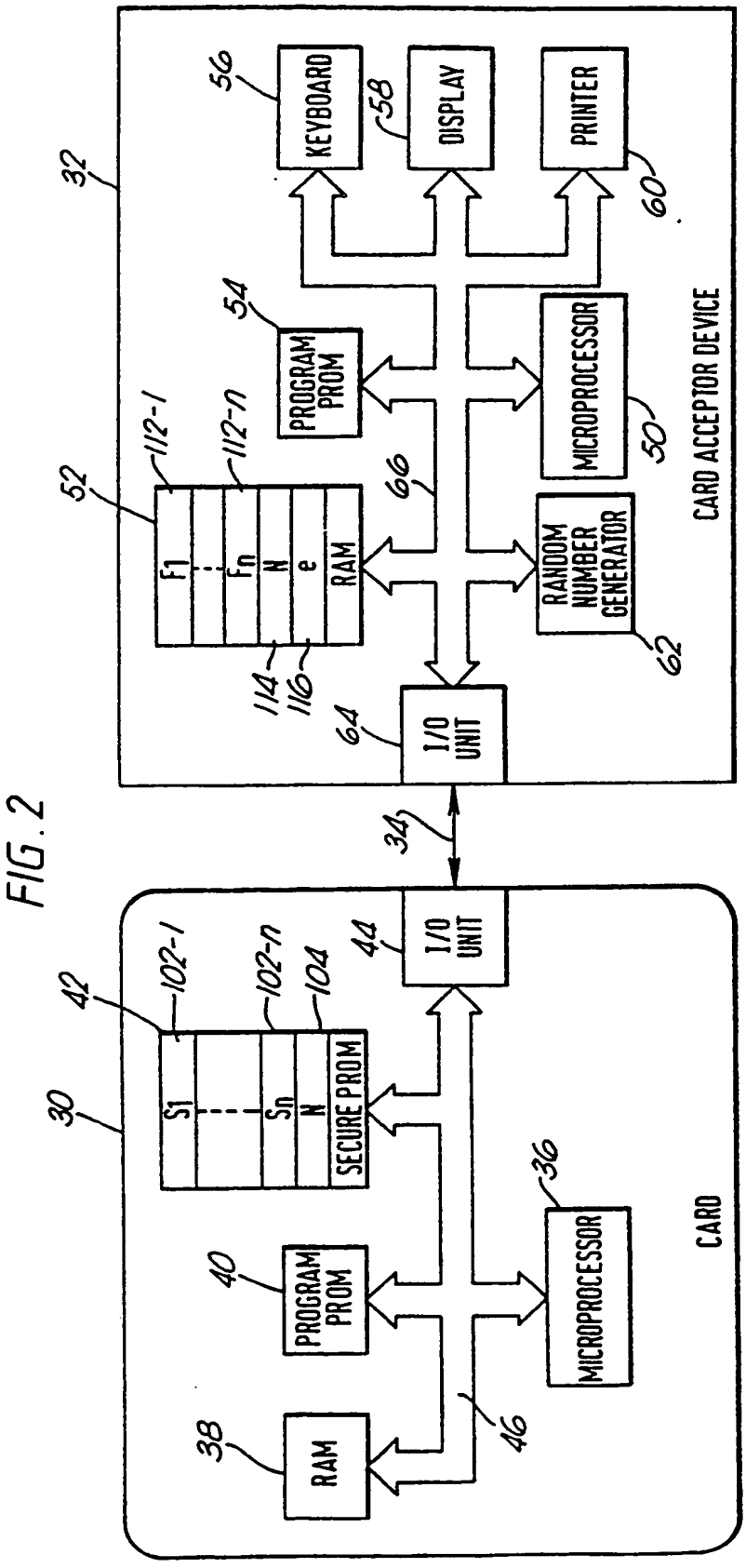

CARD ACCEPTOR DEVICE
32
KEYBOARD
56
DISPLAY
58
PRINTER
60
PROGRAM PROM
54
MICROPROCESSOR
50
52
112-1
112-n
F1
Fn
N
e
RAM
66
RANDOM NUMBER GENERATOR
62
114
116
64
I/O UNIT
34
CARD
30
42
102-1
102-n
104
S1
Sn
N
SECURE PROM
44
I/O UNIT
40
PROGRAM PROM
36
MICROPROCESSOR
38
RAM
46

FIG. 2

FIG. 3

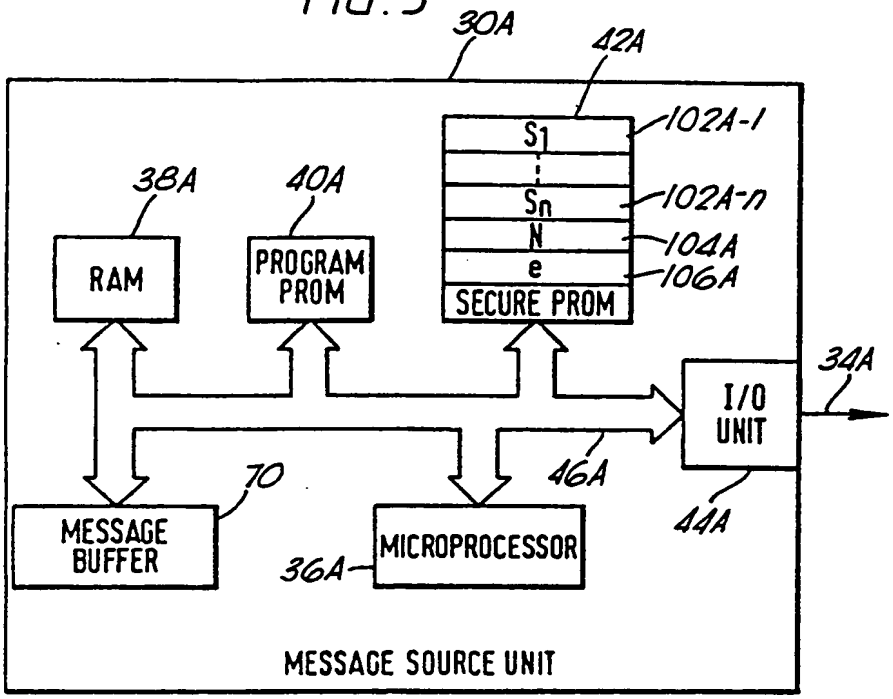
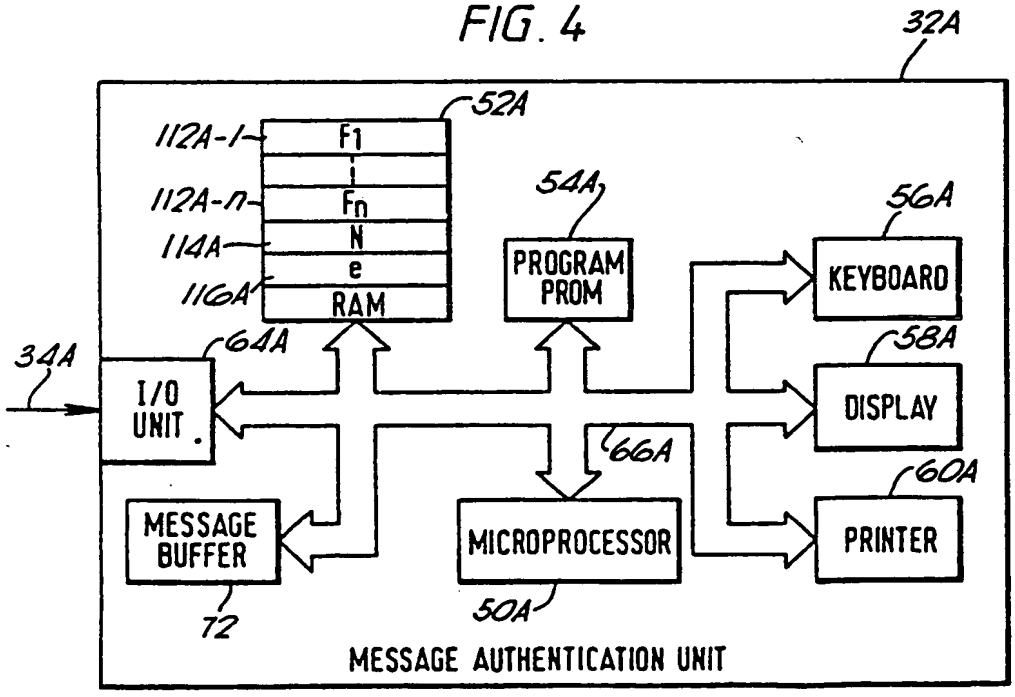

30A
42A
S1
Sn
N
e
SECURE PROM
102A-1
102A-n
104A
106A
38A
40A
RAM
PROGRAM PROM
34A
I/O UNIT
44A
46A
70
MESSAGE BUFFER
36A
MICROPROCESSOR
MESSAGE SOURCE UNIT

FIG. 4


32A
52A
112A-1
F1
112A-n
Fn
114A
N
116A
e
RAM
54A
PROGRAM PROM
56A
KEYBOARD
34A
64A
I/O UNIT
58A
DISPLAY
66A
60A
MESSAGE BUFFER
MICROPROCESSOR
PRINTER
72
50A
MESSAGE AUTHENTICATION UNIT

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 89/01944

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[4]: G 07 F 7/10, H 04 L 9/00

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[4]	G 07 F, H 04 L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
Y	US, A, 4549075 (SAADA et al.) 22 October 1985, see abstract; figure 1; column 2, line 59 - column 4, line 42; column 5, line 11 - column 7, line 14; column 8, line 1 - column 10,line 19; claims 1-7 --	1-21
Y	US, A, 4405829 (RIVEST et al.) 20 September 1983, see the whole document --	1-21
A	US, A, 4351982 (MILLER et al.) 28 September 1982, see abstract; figures 1,2; column 2, line 3 - column 6, line 26; column 7, line 52 - column 10, line 39; claims 1-12,21 --	1-21
A	US, A, 4349695 (MORGAN et al.) 14 September 1982, see abstract; figures 2-4; column 2, lines 21-32; column 4, line 31 - column 8, line 48; claims 1,2 --	1-3,5-11, 13-16,20-22

./.

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
31st August 1989	02 OCT. 1989
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	T.K. WILLIS

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No
A	US, A, 4679236 (DAVIES) 7 July 1987, see abstract; figure 6; column 1, line 63 - column 3, line 66; column 6, line 27 - column 7, line 30; claims 1-19 --	1-3,5-11, 13-16, 20-22
A	EP, A, 0218305 (CHAUM) 15 April 1987, see abstract; column 4, line 1 - column 15, line 26; claims 1-6 --	1-3,5-8, 13-15,20
A	US, A, 4723284 (MUNCK et al.) 2 February 1988, see the whole document --	1,2,5,6, 13,20
A	US, A, 4408203 (CAMPBELL) 4 October 1983, see abstract; claims 1-8 --	1
P,A	US, A, 4797920 (STEIN) 10 January 1989, see the whole document --	1,5,8,15
A	17th ACM Symposium on Theory of Computing, May 1985, ACM S. Goldwasser et al.: "The knowledge complexity of interactive proof-systems", pages 291-304, see paragraphs 4.2; pages 298-300 --	1,5,8,15
P,A	ACM Transactions on Computer Systems, vol. 6, no. 4, November 1988 ACM (New York, NY, US) T. Okamoto: " A digital multisignature scheme using bijetive public-key cryptosystems", pages 432-441, see the whole article --	1
A	Computers & Security, vol. 5, no. 3, September 1986 Elsevier Science Publishers (North-Holland) (Amsterdam, NL) G.J.M. Pluimakers et al.: "Authentication: a concise survey", pages 243-250, see the whole article	1

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. US 8901944 SA 28614

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 22/09/89
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A- 4549075	22-10-85	FR-A,B	2530053	13-01-84
		DE-A-	3374039	12-11-87
		EP-A,B	0100260	08-02-84
		JP-A-	59062241	09-04-84
US-A- 4405829	20-09-83	None		
US-A- 4351982	28-09-82	AU-B-	544169	16-05-85
		AU-A-	8006982	01-07-82
		BE-A-	891490	31-03-82
		CA-A-	1173538	28-08-84
		CH-B-	660822	15-06-87
		FR-A,B	2496303	18-06-82
		GB-A,B	2101855	19-01-83
		NL-T-	8120500	01-10-82
		SE-A-	8204697	13-08-82
		WO-A-	8202129	24-06-82
US-A- 4349695	14-09-82	None		
US-A- 4679236	07-07-87	None		
EP-A- 0218305	15-04-87	US-A-	4759064	19-07-88
US-A- 4723284	02-02-88	None		
US-A- 4408203	04-10-83	US-A-	4259720	31-03-81
US-A- 4797920	10-01-89	None		

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 :		(11) Numéro de publication internationale:
H04L 9/32	A1	WO 96/33567
		(43) Date de publication internationale: 24 octobre 1996 (24.10.96)

(21) Numéro de la demande internationale: PCT/FR96/00612

(22) Date de dépôt international: 22 avril 1996 (22.04.96)

(30) Données relatives à la priorité:

95/04753	20 avril 1995 (20.04.95)	FR
95/07668	27 juin 1995 (27.06.95)	FR

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

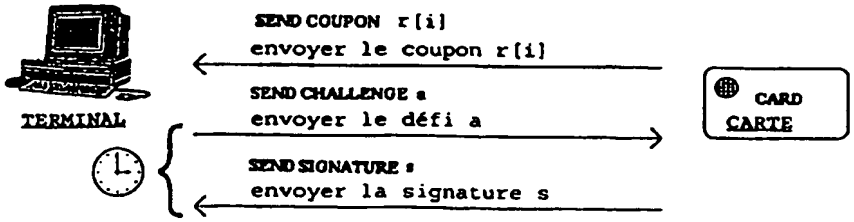
(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS [FR/FR]; Parc d'activités de la Plaine-de-Jouques, Avenue du Pic-de-Bertagne, F-13420 Gemenos (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR).

(74) Mandataire: BORIN, Lydie; Cabinet Ballot-Schmit, 16, avenue du Pont-Royal, F-94230 Cachan (FR).

(54) Title: PROCESS FOR GENERATING ELECTRONIC SIGNATURES, IN PARTICULAR FOR SMART CARDS

(54) Titre: PROCEDE DE GENERATION DE SIGNATURES ELECTRONIQUES NOTAMMENT POUR CARTES A PUCES



(57) Abstract

The invention concerns processes for generating digital signatures for electronic messages. The invention proposes modifying signature-generating algorithms, such as DSAs ("Digital Signature Algorithms), in order to enable smart cards with reduced calculation and storage resources to produce digital signatures with a high degree of security in spite of their reduced resources. The signature-checking terminal sends a random number *a* and measures the time taken by the card to send back a signal s using this random number. If the time is greater than a given duration, the signature is rejected even if the check of its authenticity is positive. In addition, part of the signature (the part which does not use the secret card key but only the public algorithm parameters) is precalculated and stored in the card in the form of signature portions produced by a compression function such that they are short. Only the second part of the signature has to be calculated by the card. According to the invention, the calculations to be made are simple so that the card does not require extensive calculation and memory resources.

(57) Abrégé

L'invention concerne les procédés de génération de signature numérique de messages électroniques. L'invention propose de modifier les algorithmes de génération de signature tels que DSA ("Digital Signature Algorithm") pour permettre à des cartes à puces à faibles ressources de calcul et de mémoire de produire des signatures numériques avec un haut degré de sécurité malgré leurs faibles ressources. On prévoit que le terminal de vérification de signature envoie un nombre aléatoire a et chronomètre le temps mis par la carte pour renvoyer une signature s utilisant ce nombre aléatoire. Si le temps est supérieur à une durée déterminée, la signature est rejetée même si la vérification de son authenticité est positive. D'autre part, on prévoit qu'une partie de la signature (partie qui n'utilise pas la clé secrète de la carte mais seulement des paramètres publics de l'algorithme) est précalculée et stockée dans la carte sous forme de coupons de signature obtenus par une fonction de compression de sorte qu'ils ont une faible longueur. Seule la deuxième partie de signature est à calculer par la carte, et on s'arrange pour que les calculs à effecturer soient simples pour que la carte n'ait pas besoin de ressources de calcul et de mémoire importantes.

PROCEDE DE GENERATION DE SIGNATURES ELECTRONIQUES, NOTAMMENT POUR CARTES A PUCES

L'invention concerne un procédé de génération de signatures numériques de messages électroniques.

Le procédé s'applique particulièrement à la signature de messages par des appareils portables du type carte à puce à microprocesseur.

Par exemple, il s'agit de signer des messages envoyés par la carte à un terminal de lecture ou à une autorité centrale; ou encore, il s'agit de faire une transaction (chèque électronique) et de signer cette transaction pour qu'elle puisse être authentifiée d'abord par le terminal de lecture dans lequel est faite la transaction, ensuite par une autorité centrale qui gère les transactions.

Le procédé qui va être décrit est apparenté aux algorithmes de génération de signatures numériques qui ont été publiés ces dernières années, notamment par le US National Institute of Standards and Technology, tel que l'algorithme DSA (Digital Signature Algorithm) décrit dans la demande de brevet US 07/738431 et annoncé le 30 Août 1991 au Registre Fédéral tenu par cet Institut, pages 42980-42982.

L'invention a pour but de modifier les procédés connus, notamment pour les rendre adaptables à des cartes à microprocesseur qui n'ont pas des ressources matérielles (processeur, mémoires) suffisantes pour réaliser rapidement des opérations mathématiques sur des grands nombres. Les algorithmes connus, notamment l'algorithme DSA, utilisent des grands nombres pour générer les signatures avec un degré de sécurité suffisant.

Pour mieux faire comprendre l'invention, on va d'abord rappeler ce qu'est l'algorithme DSA.

Une signature DSA est constituée par une paire {r, s} de grands nombres représentés dans les calculateurs par des chaînes longues de chiffres binaires (160 chiffres). La signature numérique est calculée à l'aide d'une série de règles de calcul, définies par l'algorithme, et d'un ensemble de paramètres utilisés dans ces calculs. La signature permet à la fois de certifier l'identité du signataire (parcequ'elle fait intervenir une clé secrète propre au signataire) et l'intégrité du message signé (parcequ'elle fait intervenir le message lui-même). L'algorithme permet d'une part de générer des signatures, et d'autre part de vérifier des signatures.

La génération de signature DSA fait intervenir une clé secrète. La vérification fait intervenir une clé publique qui correspond à la clé secrète mais ne lui est pas identique. Chaque utilisateur possède une paire de clés (secrète, publique). Les clés publiques peuvent être connues de tous, alors que les clés secrètes ne sont jamais dévoilées. Toute personne a la capacité de vérifier la signature d'un utilisateur en utilisant la clé publique de celui-ci, mais seul le possesseur de la clé secrète peut générer une signature correspondant à la paire de clés.

Les paramètres de l'algorithme DSA sont les suivants :

- un nombre premier p tel que $2^{L-1} < p < 2^{L}$ pour L compris entre 512 et 1024 (bornes comprises), et L = 64a pour un a entier quelconque;
- un nombre premier q tel que $2^{159} < q < 2^{160}$ et p-1 est un multiple de q;
- un nombre g, d'ordre q modulo p, tel que :

$g = h^{(p-1)/q}$ modulo p, où h est un entier quelconque vérifiant

$1 < h < p-1$ et $g > 1$;

- un nombre x généré aléatoirement ou pseudo-aléatoirement (c'est la clé secrète, figée pour un utilisateur donné);

- un nombre y défini par la relation

$y = g^x$ modulo p; (c'est la clé publique liée à la clé secrète); les opérations modulaires définies ci-après, modulo p ou modulo q seront désignés par mod p ou mod q respectivement;

- un nombre k généré aléatoirement ou pseudo-aléatoirement, tel que $0 < k < q$.

Les entiers p, q, et g sont des paramètres du système pouvant être publiés et/ou partagés par un groupe d'utilisateurs. Les clés, secrète et publique, d'un signataire sont respectivement x et y. Le paramètre k, aléatoire, doit être régénéré pour chaque nouvelle signature. Les paramètres x et k sont utilisés pour la génération de signatures et doivent être gardés secrets.

Afin de signer un message m (qui sera en général une valeur hachée d'un fichier initial M), le signataire calcule la signature {r, s} par :

$r = (g^k \bmod p) \bmod q$, et

$s = (m + xr)/k \bmod q$

(où la division par k s'entend modulo q, c'est-à-dire que 1/k est le nombre k' tel que $kk' = 1 \bmod q$; par exemple si q=5 et k = 3, alors 1/k = 2 car 3x2 = 6, soit 1 mod 5).

Après avoir testé que r et s sont différents de zéro, la signature {r, s} est envoyée au vérifieur. Le vérifieur est en général le terminal dans lequel est insérée la carte à puce qui envoie le message m et la signature {r, s}.

Le vérifieur, qui connaît p, q, g (liés à l'application), y (lié à l'utilisateur), et m (le message qu'il a reçu de la carte), calcule :

a. $w = (1/s) \bmod q$

b. $u1 = mw \bmod q$

c. $u2 = rw \bmod q$

d. $v = [g^{u1}.y^{u2} \bmod p] \bmod q$

Or cette valeur $[g^{u1}.y^{u2} \bmod p] \bmod q$ est justement égale à r si s a la valeur $(m + xr)/s \bmod q$.

Par conséquent, le terminal reçoit r et s et vérifie que v est bien égal à r pour accepter la signature, ou la rejeter dans le cas contraire.

Dans ce qui suit, on utilisera indifféremment les termes de signataire ou organe signataire, ou dispositif prouveur, ou de carte à puce, pour désigner le dispositif qui émet la signature et qui sera en général une carte à puce. Et on utilisera indifféremment le terme de vérifieur, ou organe vérifieur ou dispositif vérifieur, ou terminal vérifieur, ou encore autorité de contrôle, pour désigner le dispositif qui reçoit la signature et la vérifie pour accepter ou rejeter une transaction ou un message. L'application la plus simple de l'invention est l'émission d'une signature par une carte à puce vers un terminal de lecture dans lequel la carte est insérée, le terminal exécutant la fonction de vérification et étant relié ou non à une autorité centrale de gestion.

Un des buts de la présente invention est d'augmenter la sécurité de génération et vérification de signatures électroniques numériques, en minimisant les moyens de calcul et de mémoire qui doivent être présents dans la carte à puce pour produire les signatures.

Il serait en particulier souhaitable de pouvoir utiliser dans la carte des microprocesseurs peu chers à 8 bits, malgré le fait qu'ils ne peuvent pas facilement

traiter des grands nombres, plutôt que des microprocesseurs plus puissants et plus coûteux. Mais cela ne doit pas se faire au détriment de la sécurité.

Selon un premier aspect important, l'invention propose que la vérification par un vérifieur (terminal) de la signature envoyée par le signataire (carte) utilise une étape de chronométrage de la durée s'écoulant entre un instant où une donnée (en principe aléatoire) est envoyée par le vérifieur au signataire (carte) et l'instant où la signature (utilisant cette donnée aléatoire) revient au vérifieur. Si le temps écoulé est trop long, c'est que le traitement de calcul de signature par le signataire s'effectue de manière anormale et la signature est rejetée même si son authenticité est confirmée par le vérifieur.

Indirectement, cette solution permet, comme on le verra, de conserver la même sécurité de signature tout en utilisant des ressources matérielles faibles (puissance de calcul et mémoires) dans la carte à puce. Des ressources faibles entraînent la nécessité de modifier les procédés de génération et vérification de signatures, mais c'est au détriment de la sécurité. L'étape de chronométrage selon l'invention restaure un niveau de sécurité suffisant.

On décrira en détail cette solution à partir d'algorithmes dérivés de l'algorithme DSA rappelé ci-dessus, mais on comprendra que ce premier aspect de l'invention est applicable avec d'autres algorithmes même s'ils sont très différents de l'algorithme DSA.

En résumé, le premier aspect de l'invention consiste dans un procédé de signature électronique, comportant la génération d'une signature numérique par un organe signataire qui calcule cette signature en utilisant une donnée aléatoire envoyée par un organe vérifieur, et la vérification de la signature par le

vérifieur qui vérifie si une condition mathématique faisant intervenir la signature envoyée et la donnée aléatoire est remplie, ce procédé étant caractérisé en ce que la vérification de la signature envoyée par le signataire au vérifieur utilise en outre une étape de chronométrage de la durée s'écoulant entre un instant où la donnée aléatoire est envoyée par le vérifieur au signataire et l'instant où la signature utilisant cette donnée revient au vérifieur après calcul par le signataire, la signature étant acceptée si le temps écoulé est inférieur à une seuil déterminé et si la condition mathématique est vérifiée.

De préférence, l'algorithme utilisé est du type dans lequel la génération de signature produit deux valeurs {r, s}, s étant calculée à partir de r et d'une clé secrète x, et dans lequel la vérification de la signature {r, s} consiste dans la vérification d'une égalité v = f(r, s) = r entre r et une fonction f de r et de s. On prévoit alors selon l'invention que la fonction f est choisie suffisamment complexe pour que la durée de recherche d'une valeur s à partir de cette égalité en l'absence de connaissance de la clé secrète soit très supérieure, même si elle est faite par un calculateur puissant, à la durée de calcul et transmission par la carte de la valeur s à partir de r et de la clé secrète, et ceci même si la carte utilise un microprocesseur peu puissant (microprocesseur de 8 bits à 20 MHz par exemple). Ainsi, en choisissant correctement la condition de temps introduite par le chronométrage, on fait en sorte que cette condition ne puisse pas être remplie en l'absence de connaissance de la clé secrète et notamment ne puisse pas être remplie par une recherche de s à partir de l'égalité r = f(r, s).

En pratique, la fonction f(r, s) fait intervenir aussi un message m à signer, de sorte qu'on peut la noter f(r, s, m).

De préférence, la fonction f comporte des calculs mathématiques suivis d'une fonction de hachage complexe. La première partie de signature r est établie par d'autres calculs mathématiques, suivis de la même fonction de hachage complexe.

Cette fonction de hachage complexe est de préférence, comme on l'expliquera plus loin, une fonction de compression complexe aboutissant à une réduction de la longueur des chaînes de bits obtenues par les calculs mathématiques effectués.

On rappelle qu'une fonction de hachage est une fonction de traitement logique de chaînes binaires, qui permet d'obtenir une chaîne de caractères de longueur déterminée à partir d'une autre chaîne de caractères de même longueur ou de longueur différente. Une fonction de hachage complexe peut être obtenue par des hachages successifs et/ou des calculs mathématiques impliquant les résultats de plusieurs hachages. Une compression peut être obtenue à la fin en prenant comme résultat une valeur modulaire, modulo 2^e, où e est la longueur de la chaîne finalement désirée.

Par ailleurs, selon un autre aspect important de l'invention, on propose une nouvelle solution pour traiter des plus petits nombres dans la carte à puce, dans des algorithmes de signature numérique du genre dans lequel la signature fait intervenir deux nombres, r et s, seul le nombre s faisant intervenir la clé secrète de la carte et le message à envoyer.

Ce deuxième aspect de l'invention est un perfectionnement à un procédé de génération de signatures qui a été décrit dans la demande de brevet français 93 14466. Dans cette demande de brevet, il est expliqué que

dans un algorithme de ce genre (DSA en est un exemple), le nombre r ne dépend ni du message m envoyé par la carte, ni de la clé secrète contenue dans la carte. Il ne dépend que de nombres figés pour l'application considérée, et de nombres aléatoires; par exemple, ces nombres sont g, p, q et k dans l'algorithme DSA. Il est donc inutile de faire calculer r par la carte, car cela consomme un temps de calcul important. On fait plutôt calculer à l'avance par une autorité centrale certifiée une série de n valeurs r possibles, notées r_i, i étant un indice allant de 1 à n. On stocke les valeurs r_i dans la carte. A chaque nouvelle utilisation de la carte, on utilise une des valeurs r_i (et on n'utilisera plus cette valeur les fois suivantes). Au moment de signer, la carte calcule seulement l'autre partie de signature s, à partir d'une valeur r_i, de la clé secrète x, du message m, et on envoie au vérifieur le message m et le couple $\{ r_i, s\}$ représentant la signature que le vérifieur peut alors vérifier de la manière prévue par l'algorithme considéré.

Les nombres r_i sont des certificats précalculés, appelés encore des "coupons de signature". Ils constituent une partie seulement de la signature à envoyer, et ils peuvent être préparés et stockés à l'avance dans la carte. L'indice i représente l'indice de coupon utilisé lors d'une signature donnée.

Mais une des difficultés réside dans la grande longueur de ces coupons (160 bits dans l'algorithme DSA présenté ci-dessus). Ils consomment une place importante de mémoire non volatile dans la carte; on ne peut pas en sauvegarder un grand nombre dans la carte si on dispose d'une taille limitée de mémoire non volatile; et en plus, ils entraînent un plus long temps de calcul avec un microprocesseur 8 bits puisqu'il faut aller chercher ces nombres par petits morceaux. Mais si on utilisait et stockait des plus petits coupons de signature, la

garantie d'authenticité de signature risquerait d'être bien plus faible.

L'invention décrite ici permet de concilier le souci d'une garantie d'authenticité avec l'utilisation de plus petits coupons de signature r_i.

L'invention propose donc un procédé de génération de signature électronique par un organe signataire et de vérification par un organe vérifieur, utilisant un algorithme de signature numérique dans lequel la signature envoyée par le signataire comprend au moins un coupon de signature r_i et un complément de signature s qui est calculé à partir du coupon r_i et d'une clé secrète x de la carte, cet algorithme permettant la vérification de signature par un vérifieur à l'aide d'une formule de vérification du type

$$v = f(r_i, s) = r_i,$$

ce procédé étant caractérisé en ce que

a. le coupon de signature est établi à l'avance par une autorité certifiée, en deux étapes :

- calcul d'un nombre représenté par une chaîne binaire longue, à l'aide d'une formule mathématique faisant intervenir des grands nombres binaires;

- et modification du résultat de ce calcul par une fonction de compression complexe réduisant fortement la longueur de ce résultat,

b. une série de coupons différents de faible longueur sont ainsi préparés à l'avance et stockés dans l'organe signataire (carte à puce à mémoire et microprocesseur),

c. la génération de signature comporte l'envoi d'un coupon r_i et d'un complément de signature s calculé à partir d'au moins r_i et x,

d. l'algorithme de vérification de signature comporte un calcul mathématique suivi de la même fonction

de compression complexe que celle qui a servi à l'élaboration du coupon, et le résultat est comparé au coupon pour la vérification de signature.

La fonction de compression est de préférence une fonction de hachage complexe qui nécessite un temps de calcul assez long. Ceci donne une sécurité importante au procédé de génération et de vérification de signature. On combine donc l'avantage d'une bonne garantie d'authenticité de signature avec la possibilité de ne sauvegarde dans la carte que des coupons de petite taille, donc la possibilité d'en sauvegarde beaucoup. Si de surcroît on utilise le chronométrage mentionné plus haut, on conçoit qu'on peut renforcer à un très haut degré la garantie d'authenticité.

Le calcul de la signature s fait bien sûr intervenir le message m qu'on veut signer, pour garantir non seulement l'authenticité de la signature mais aussi l'intégrité du message transmis.

On peut encore améliorer la sécurité par une ou plusieurs des caractéristiques suivantes :

La formule de calcul du coupon r_i est de préférence établie à partir d'un aléa J engendré au départ par la carte et stocké dans la carte pour être réutilisé lorsque le coupon sera utilisé pour l'établissement d'une signature.

On peut prévoir que pour déclencher la génération d'une signature, le terminal vérifieur envoie un aléa *a* à la carte et déclenche alors le chronomètre; on prévoit aussi que l'établissement du complément de signature utilise nécessairement cet aléa *a* et que la vérification de signature nécessite également cet aléa *a*.

Le complément de signature s est de préférence établi par un calcul faisant intervenir une fonction de hachage SHA(m, a) du message et de cet aléa *a*, la même

fonction de hachage étant utilisée pour la vérification de signature.

Le complément de signature s est de préférence établi par un calcul faisant intervenir un aléa J stocké dans la carte et ayant servi à établir le coupon de signature. De préférence encore, ce calcul de s fait intervenir une fonction de hachage SHA(x, J, i) portant sur cet aléa J et sur un indice i représentant le numéro du coupon utilisé, cette même fonction de hachage ayant été précédemment utilisée au cours du calcul de chaîne binaire longue prévu dans le calcul du coupon correspondant. Cette fonction de hachage fait de préférence aussi intervenir la clé secrète x de la carte.

Le complément de signature s est de préférence établi par un calcul faisant intervenir une fonction de hachage du coupon $SHA(r_i)$, la même fonction de hachage $SHA(r_i)$ étant utilisée pour la vérification de signature.

Ainsi, selon un aspect particulier de l'invention, on propose un procédé de génération de signatures numériques de messages par un dispositif signataire et de vérification de ces signatures par un dispositif vérifieur, le dispositif signataire comportant des moyens de calcul, de communication et de rétention de données comprenant au moins une mémoire non volatile programmable électriquement, selon lequel on prépare des données chiffrées constituant des coupons de signature r_i que l'on charge dans la mémoire non-volatile et que le dispositif signataire utilise pour signer des messages, principalement caractérisé en ce que :

- les coupons sont compressés par application d'une fonction de compression, dite encore fonction de hachage, par une autorité certifiée avant d'être chargés dans la mémoire, et en ce qu'il comporte les échanges suivants :

- un message m est transmis et ce message doit être certifié par une signature;

- le signataire envoie un coupon r_i au vérifieur,

- le vérifieur envoie un nombre aléatoire a au signataire et déclenche un chronomètre,

- le signataire calcule la signature s du message et l'envoie au vérifieur,

- le vérifieur arrête le chronomètre et vérifie que la signature a été obtenue par le secret détenu dans la carte et le coupon r_i reçu; cette vérification est faite en vérifiant l'égalité suivante :

$$v = f(r_i, s, m) = r_i$$

- le vérifieur accepte la signature si la condition de vérification $v = r_i$ est remplie et si le temps chronométré ne dépasse pas une durée prédéterminé impartie.

Pour simplifier, dans toute la suite on parlera surtout de carte pour le signataire ou signataire.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit et qui est faite en référence aux dessins annexés dans lesquels :

- la figure 1 décrit l'organigramme d'une carte mettant en oeuvre le système proposé par la présente invention;

- la figure 2 décrit les données transmises entre la carte et le terminal au moment de l'utilisation du coupon;

- la figure 3 décrit l'organigramme d'un terminal mettant en oeuvre le système proposé par la présente invention;

- la figure 4 représente les données transmises entre la carte et l'autorité pendant la phase de

chargement des coupons et l'organisation de la mémoire d'une carte après le chargement de n coupons.

A partir des explications données en préambule, on aura compris que le principal avantage des coupons de signature précalculés selon la méthode de l'invention réside dans la vitesse de calcul d'une signature par une carte basée sur un simple microcontrôleur de 8 bits et le faible taux d'occupation de mémoire des coupons stockés. Typiquement le calcul de signature peut se faire en 300ms environ, temps de transmission compris, et chaque coupon peut utiliser de deux à quatre octets de mémoire EPROM ou EEPROM.

On va décrire l'invention dans cet exemple, étant entendu que ce n'est qu'un exemple, bien qu'il soit considéré ici comme le plus avantageux.

Le procédé de génération de signatures se décompose dans ce cas en deux phases distinctes : le chargement des coupons par l'autorité ayant délivré la carte, puis l'utilisation de ces coupons par la carte, face à un terminal ne connaissant pas le secret x de la carte.

Les deux phases font ici appel à des fonctions de hachage de deux types différents. On rappelle qu'une fonction de hachage d'un nombre, représenté par une chaîne de bits, consiste en la production d'une autre chaîne de bits de longueur déterminée, longueur qui est ou non la même que celle de la chaîne de départ, et ceci à partir de fonctions logiques exécutées sur des groupes de bits de la chaîne de départ.

Des fonctions de hachage simples sont utilisées, notées SHA(ch) pour le hachage d'une chaîne ch. Ces fonctions peuvent être des fonctions de hachage classiques, telles que celles publiées dans la récente norme américaine SHA (Secure Hash Algorithm - FIPS PUB

XX, du 1er Février 1993, dans "Digital Signature Standard"). Ces fonctions peuvent être la fonction MDA ou MD5 ou un hachage basé sur l'algorithme DES (Data Encryption Standard).

D'autres fonctions, dites hachage complexe, seront utilisées aussi. Leur caractéristique utilisée ici n'est pas tant d'être une fonction de hachage que d'être une fonction de ralentissement imposée lors de certains traitements de signaux, et aussi d'être une fonction de compression réduisant la longueur des coupons de signature qu'on veut sauvegarde dans la carte à puce.

Cette fonction de ralentissement et de compression est notée ci-après H(ch) pour le traitement d'une chaîne ch.

Toutes sortes de fonctions de ralentissement et compression pourraient être utilisées dans l'invention. A titre d'exemple on a pris comme fonction H(ch) la fonction suivante, où SHA(ch) désigne une fonction de hachage classique :

$$H(ch) = SHA[SHA\{SHA(ch)\}^{SHA(ch)} \bmod p] \bmod 2^e ,$$

où e est la longueur désirée pour les coupons, par exemple 16 à 40 bits soit quelques octets.

Dans tout ce qui suit, on reprendra un algorithme directement inspiré de l'algorithme DSA, pour montrer comment on met en oeuvre les particularités originales de l'invention. Les paramètres p, q, g, x, y utilisés sont ceux définis précédemment à propos de l'algorithme DSA.

CHARGEMENT DE COUPONS DANS LA CARTE

C'est l'étape préliminaire, mais bien sûr seulement dans le cas où on calcule à l'avance, en dehors de la carte, la première partie r de la signature {r, s}

et où on charge plusieurs valeurs possibles r_i dans la carte.

1. La carte remet à zéro un compteur en mémoire non volatile (EPROM ou EEPROM), génère un aléa J (de 10 à 20 octets par exemple), l'enregistre en mémoire non-volatile, et l'envoie à l'autorité de contrôle qui connaît le secret x de la carte et qui calcule, pour i = 1 à n, plusieurs valeurs k_i et plusieurs valeurs r_i :

$$k_i = \{1/(SHA(x, J, i)\} \bmod q$$

et $r_i = H(g^{ki} \bmod p)$; H est la fonction de ralentissement et de compression.

On pourrait envisager aussi que la carte calcule pour chaque i la valeur SHA(x, J, i) et l'envoie à l'autorité de contrôle; celle-ci calcule les nombres r_i.

2. L'autorité envoie les nombres r_i à la carte qui les stocke en mémoire, en conservant le lien avec le repère i. Les nombres k_i ne sont pas conservés.

Si on se réfère à l'algorithme DSA, k_i représente le nombre k aléatoire, modifié à chaque nouvelle signature. Mais au lieu d'être émis par le terminal vérifieur au moment d'une signature, il sera recalculé au moment opportun par la carte. Comme il dépend de i et qu'un coupon d'indice i n'est utilisé qu'une fois, k_i est renouvelé à chaque fois.

UTILISATION D'UN COUPON POUR SIGNER UN MESSAGE

Lorsque la carte désire signer un message, le protocole suivant est utilisé après transmission du message m (de préférence sous forme de fonction hachée du

véritable message, selon une fonction de hachage connue du terminal qui reçoit le message) :

1. La carte

- extrait l'état i du compteur (représentant l'indice courant de la signature qui va être produite),
- extrait de la mémoire non volatile l'aléa J, le secret x, le coupon r_i correspondant à l'indice i;
- calcule I = SHA(x, J, i); cette valeur I n'est autre que l'inverse modulaire de k_i qui a servi au calcul du coupon r_i ;
- calcule A = $xSHA(r_i) \bmod q$
- incrémente i (pour une prochaine signature)
- envoie r_i au terminal vérifieur; cet envoi représente la première partie de la signature.

2. Le terminal génère alors un aléa a, pour déclencher la génération de la deuxième partie de signature s; cet envoi constitue en quelque sorte le lancement d'un défi à la carte car le terminal vérifieur déclenche en même temps un chronomètre pour mesurer le temps de réponse de la carte à ce défi.

La signature s que la carte doit envoyer, compte tenu de la formule de vérification $f(r_i, m, s, a) = r_i$ qui est prévue dans le vérifieur est

$$s = [xSHA(r_i) \bmod q + SHA(m, a)] / k_i \bmod q$$

Cette formule fait intervenir le coupon r_i, le secret x de la carte, le message m envoyé, le nombre k_i, et l'aléa a envoyé par le vérifieur à titre de défi. Cette formule est différente de celle qui a été donnée pour l'algorithme DSA : $s = (m + xr)/k$ pour plusieurs

raisons : elle doit faire intervenir l'aléa *a* envoyé à titre de défi, pour que le vérifieur soit sûr que le calcul chronométré de signature s ne commence que lorsque l'aléa *a* est parvenu à la carte. C'est pour cela qu'on utilise un hachage de m et de l'aléa *a*, SHA (m, a), au lieu de m. D'autre part on utilise de préférence $SHA(r_i)$ plutôt que r_i pour utiliser une valeur de coupon sous forme de chaîne plus longue que r_i qui est une chaîne très courte. Ceci renforce la sécurité. Mais bien entendu, si on utilise $xSHA(r_i)$ au lieu de xr_i et SHA(m, a) au lieu de m, la formule de vérification doit en tenir compte, et on verra plus loin que c'est ce qui est fait. D'autres variantes de calcul de signature peuvent être prévues, à condition simplement que la formule de vérification en tienne compte.

3. La carte calcule, aussi vite que possible, la signature s. Mais comme elle a déjà calculé, avant déclenchement du chronomètre, $A = xSHA(r_i) \bmod q$ et $I = 1/k_i = SHA(x, J, i)$ il ne lui reste qu'à calculer

$$s = I.(SHA(m, a) + A) \bmod q$$

Ce calcul peut être rapide même pour un microcontrôleur simple et peu coûteux de 8 bits, par exemple type 8051 de Intel ou 6805 de Motorola. Dès que le calcul est terminé, la carte renvoie la signature s.

4. Dès réception de s, le terminal arrête le chronomètre et effectue les calculs de vérification de l'authenticité de la signature. Si la signature a été correctement calculée selon la formule ci-dessus, alors on peut vérifier qu'on doit avoir l'égalité suivante :

$$[y^{(SHA(ri)/s) \bmod q} \; g^{(SHA(m, a)/s) \bmod q} \bmod p] = g^{ki} \bmod p$$

Le vérifieur ne possède pas k_i. Il possède $r_i = H(g^{ki} \bmod p)$; H est la fonction de ralentissement et de compression.

L'égalité doit donc être transformée en :

$$H[y^{(SHA(ri)/s) \bmod q} \; g^{(SHA(m,a)/s) \bmod q} \bmod p] = H(g^{ki} \bmod p) = r_i$$

Le vérifieur dispose de r_i, de s, de q, de p, de g, de m, de a, de la fonction de hachage simple SHA, et de la fonction de ralentissement et de compression H. Il vérifie donc l'égalité ci-dessus.

Si l'égalité est obtenue et si la signature a été renvoyée dans un délai inférieur à un seuil déterminé, la signature est acceptée par le vérifieur. Si une des deux conditions n'est pas remplie, elle n'est pas acceptée.

A titre d'exemple pour l'évaluation de la durée on peut donner les indications suivantes : appelons T le temps nécessaire pour évaluer H(ch) sur un ordinateur extrêmement puissant, voire le plus puissant qu'on connaisse aujourd'hui. On peut considérer que la fonction de ralentissement H, aboutissant à des chaînes de longueur e (H ayant également une fonctionnalité de compression) est suffisamment complexe, et en tous cas doit être choisie suffisamment complexe, pour que pour toute valeur z et tout ordinateur existant, la recherche d'une nouvelle valeur ch' telle que $z = H(ch')$ nécessite un temps $T.2^e$.

Etant donné que quelqu'un qui ignore le secret de la carte ne peut rechercher s que par tâtonnements à partir de la formule de vérification (recherche exhaustive), il ne pourra pas, même avec un seul essai, trouver une valeur correcte de s si on choisit de mettre un seuil de durée de renvoi de signature très inférieur à

cette valeur $T.2^e$, par exemple 1 millionième de cette valeur.

Ceci donne une indication de la méthodologie à suivre pour choisir la fonction de ralentissement H et la durée de seuil.

De façon générale, les principes qui ont été expliqués ci-dessus et illustrés par un exemple sont applicables à d'autres protocoles de signature. En particulier ils sont applicables à d'autres protocoles dans lesquels un précalcul de coupons de signature est possible, en particulier les protocoles suivants :

- Rueppel-Nyberg : "New signature schemes based on the discrete logarithm problem" publié dans les actes du colloque Eurocrypt 94.
- Schnorr : "Efficient identification and signatures for smart-cards", publié dans les actes du colloque Crypto'89.
- El-Gamal : "A public-key cryptosystem and a signature scheme based on discrete logarithms" publié dans la revue IEEE Transactions on Information Theory, vol IT30, n°4, pages 469-472.
- Guillou-Quisquater : "A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory", publié dans les actes du colloque Eurocrypt'88 et "A paradoxical identity-based signature scheme resulting from zero-knowledge", publié dans les actes du colloque Crypto'88.
- d'autres systèmes à clé publique basés sur le logarithme discret, où l'équation $(m + xr)/k \bmod q$ est remplacée par une autre égalité faisant intervenir m, x, r, et k (comme expliqué dans l'article "Meta Message Recovery and Meta Blind Signature schemes based on the discrete logarithm problem and their applications", publié par Horster et al. dans les actes du colloque

Asiacrypt'94) ou encore en utilisant plusieurs aléas distincts k ou plusieurs secrets distincts x dans la même signature.

L'invention est applicable à la signature de chèques électroniques et permet alors de faire de tels chèques avec des cartes à puces à faible coût (résultant de l'utilisation d'un microprocesseur de 8 bits et d'une mémoire non volatile de taille limitée).

En effet, le message m peut représenter une transaction effectuée par la carte avec le terminal qui est par exemple le terminal de paiement d'un commerçant. Ce message m est signé. Le terminal vérifie la signature pour accepter le message, donc la transaction, mais ce terminal est également relié à une autorité centrale de gestion (une banque par exemple) qui doit pouvoir elle-même contrôler le message et l'authenticité de la signature avant de débiter le compte du signataire d'une part et/ou créditer le compte du commerçant d'autre part.

Ainsi, après avoir exécuté toute la procédure de signature et vérification de signature décrite en détail ci-dessus, le terminal envoie à l'autorité de contrôle le chèque électronique $\{i, r_i, a, s, m\}$, et l'autorité s'assure que la signature s est la bonne signature, c'est-à-dire que :

$$s = SHA(x, J, i)[SHA(m, a) + xSHA(r_i)] \bmod q$$

et l'autorité crédite le compte du terminal du montant de la transaction définie dans le message m.

On notera que dans le calcul de la signature par la carte, on peut utiliser l'expression SHA(m, i, a) au lieu de SHA(m, a). Auquel cas il faut bien sûr que la formule de vérification par le terminal en tienne compte et soit donc :

$$H[y^{(SHA(ri)/s) \bmod q}\, g^{(SHA(m, i, a)/s) \bmod q} \bmod p] = r_i$$

et que la formule de vérification de signature par l'autorité en tienne compte également et soit :

$$s = SHA(x, J, i)[SHA(m, i, a) + xSHA(r_i)] \bmod q$$

Si on se réfère aux figures, chaque carte à puce se compose d'une unité de traitement (CPU) 11, d'une interface de communication 10, une mémoire vive 13 (RAM) et/ou une mémoire non inscriptible (ROM) 14 et/ou une mémoire non volatile inscriptible ou réinscriptible (EPROM ou EEPROM) 15.

L'unité de traitement 11 et/ou la ROM 14 de la carte à puce contiennent des programmes ou des ressources de calcul correspondant à l'exécution des étapes de calcul effectuées par la carte lors du chargement des coupons et lors de la signature d'un message ou l'émission d'un chèque électronique. Ces programmes comportent notamment les règles de calcul pour la génération de s et les règles d'utilisation de la fonction de hachage SHA. L'unité de calcul et les programmes en ROM comportent également les ressources nécessaires à des multiplications, additions et réductions modulaires. Certaines de ces opérations peuvent être regroupées (par exemple, la réduction modulaire peut être directement intégrée dans la multiplication).

De même que pour l'algorithme DSA, la RAM de la carte contient le message M et l'aléa a sur lesquels s'applique la fonction de hachage SHA(m, a) ou SHA(m, i, a) par exemple. La mémoire non volatile 15 contient typiquement les paramètres q, x, J et le jeu de coupons (r_i) précalculés. L'indice i est dans un compteur non volatile incrémenté à chaque nouvelle génération de signature et remis à zéro lors du chargement de coupons.

L'unité de traitement de la carte commande, via des bus d'adresses et de données 16 et l'interface de

communication 10, les opérations de lecture et d'écriture en mémoire 13, 14, et 15.

Chaque carte à puce est protégée du monde extérieur par des protections physiques 17. Ces protections devraient être suffisantes pour empêcher toute entité non autorisée d'obtenir la clé secrète x. Les techniques les plus utilisées de nos jours en la matière sont l'intégration de la puce dans un module de sécurité et l'équipement des puces de dispositifs capables de détecter des variations de température, de lumière, ainsi que des tensions et fréquences d'horloge anormales. Des techniques de conception particulières telles que l'embrouillage de l'accès mémoire sont également utilisées.

Le terminal se compose quant à lui au minimum d'une unité de traitement (CPU) 30 et des ressources mémoires 32, 33, 34.

Le CPU 30 commande, via les bus d'adresse et de données 35 et l'interface de communication 31, les opérations de lecture et d'écriture dans les mémoires 32, 33, 34.

Le CPU 30 et/ou la ROM 34 de l'autorité contiennent des programmes ou ressources de calcul permettant de mettre en oeuvre les règles de calcul et fonctions de hachage, ralentissement et compression, multiplication, addition, inversion modulaire, exponentiation et réduction modulaire, nécessaires au calcul des coupons et à la vérification de signature. Certaines de ces opérations peuvent être regroupées (multiplication et réduction modulaire par exemple).

L'ensemble de l'invention a été décrite a propos de cartes à puces, mais on comprendra qu'elle est applicable lorsque l'organe signataire est un autre objet, et en particulier un objet portable tel que des cartes PCMCIA qui sont des sortes de cartes à puce à

protocoles de transmission parallèle et non série, ou des badges, des cartes sans contacts, etc. La communication peut s'effectuer entre la carte et le terminal soit directement par des signaux électroniques, soit par transmission à distance, hertzienne ou infrarouge.

REVENDICATIONS

1. Procédé de signature électronique, comportant la génération d'une signature numérique (s) par un organe signataire qui calcule cette signature en utilisant une donnée aléatoire (a) envoyée par un organe vérifieur, et la vérification de la signature par le vérifieur qui vérifie si une condition mathématique faisant intervenir la signature envoyée et la donnée aléatoire est remplie, caractérisé en ce que la vérification de la signature envoyée par le signataire au vérifieur utilise en outre une étape de chronométrage de la durée s'écoulant entre un instant où la donnée aléatoire est envoyée par le vérifieur au signataire et l'instant où la signature utilisant cette donnée revient au vérifieur après calcul par l'organe signataire, la signature étant acceptée si le temps écoulé est inférieur à une seuil déterminé et si la condition mathématique est vérifiée.

2. Procédé selon la revendication 1, caractérisé en ce que le calcul de la signature et la vérification sont effectués à partir d'un algorithme du type dans lequel la génération de signature produit deux valeurs {r, s}, s étant calculée par le signataire à partir de r et d'une clé secrète x, et dans lequel la vérification de la signature {r, s} consiste dans la vérification d'une égalité v = f(r, s) = r entre r et une fonction f de r et de s, et en ce que la fonction f est choisie suffisamment complexe pour que la durée de recherche d'une valeur s à partir de cette égalité en l'absence de connaissance de la clé secrète x soit très supérieure, même si elle est faite par un calculateur puissant, à la durée de calcul et de transmission par la carte de la valeur s à partir

de r et de la clé secrète, et ceci même si la carte utilise un microprocesseur peu puissant.

3. Procédé selon la revendication 2, caractérisé en ce que la fonction f(r, s) fait intervenir aussi un message m à signer.

4. Procédé selon l'une des revendications 2 et 3, caractérisé en ce que la fonction f comporte des calculs mathématiques suivis d'une fonction de hachage complexe (H) réalisant à la fois un ralentissement de l'obtention d'un résultat de calcul et une compression de longueur de ce résultat.

5. Procédé selon la revendication 4, caractérisé en ce que la première partie de signature r est établie par d'autres calculs mathématiques, suivis de la même fonction de hachage complexe (H).

6. Procédé de génération de signature et de vérification selon l'une des revendications 1 à 5, caractérisé en ce que la signature envoyée par le signataire comporte au moins un coupon de signature r_i et un complément de signature s qui est calculé à partir du coupon r_i et d'une clé secrète x de la carte, le procédé permettant la vérification de signature par le vérifieur à l'aide d'une formule de vérification du type

$$v = f(r_i, s) = r_i,$$

ce procédé étant caractérisé en ce que

a. le coupon de signature est établi à l'avance par une autorité certifiée, en deux étapes :

- calcul d'un nombre représenté par une chaîne binaire longue, à l'aide d'une formule mathématique faisant intervenir des grands nombres binaires;

- et modification du résultat par une fonction de compression complexe réduisant fortement la longueur de ce résultat,

b. une série de coupons différents de faible longueur sont ainsi préparés à l'avance et stockés dans l'organe signataire,

c. la génération de signature comporte l'envoi d'un coupon r_i et d'un complément de signature s calculé à partir de r_i, et x,

d. la vérification de signature comporte un calcul mathématique suivi de la même fonction de compression complexe que celle qui a servi à l'élaboration du coupon, et le résultat est comparé au coupon pour la vérification de signature.

7. Procédé de génération de signature électronique pouvant utiliser une étape de chronométrage selon la revendication 1, ce procédé comportant la génération d'une signature par un organe signataire et la vérification de la signature par un organe vérifieur, caractérisé en ce que la signature envoyée par le signataire comprend au moins un coupon de signature r_i et un complément de signature s qui est calculé à partir du coupon r_i et d'une clé secrète x de la carte, la vérification de signature par le vérifieur étant effectuée à l'aide d'une formule de vérification du type $v = f(r_i, s) = r_i$, et en ce que :

a. le coupon de signature est établi à l'avance par une autorité certifiée, en deux étapes :

- calcul d'un nombre représenté par une chaîne binaire longue, à l'aide d'une formule mathématique faisant intervenir des grands nombres binaires;

- et modification du résultat par une fonction de compression complexe réduisant fortement la longueur de ce résultat,

b. une série de coupons différents de faible longueur sont ainsi préparés à l'avance et stockés dans l'organe signataire,

c. la génération de signature comporte l'envoi d'un coupon r_i et d'un complément de signature s calculé à partir d'au moins r_i et x,

d. la vérification de signature comporte un calcul mathématique suivi de la même fonction de compression complexe que celle qui a servi à l'élaboration du coupon, et le résultat est comparé au coupon pour la vérification de signature.

8. Procédé selon la revendication 7, caractérisé en ce que la fonction de compression est une fonction de hachage complexe.

9. Procédé selon l'une des revendications 7 et 8, caractérisé en ce que le calcul du coupon est effectué à partir d'un aléa (J) engendré au départ par la carte et stocké dans la carte pour être réutilisé lorsque le coupon sera utilisé pour l'établissement d'une signature.

10. Procédé selon l'une des revendications 7 à 9, caractérisé en ce que, pour déclencher la génération de signature par la carte, l'organe vérifieur envoie un aléa a à la carte, déclenche alors un chronomètre, mesure le temps mis par la carte pour renvoyer le complément de signature s calculé à partir d'au moins l'aléa a et la clé secrète x de la carte, effectue un calcul de vérification de signature à partir d'au moins la signature s et l'aléa a, et accepte la signature si le calcul vérifie une condition prédéterminée et si le temps

mis par la carte pour renvoyer la signature s utilisant l'aléa a est inférieur à un seuil prédéterminé.

11. Procédé selon l'une des revendications 7 à 10, caractérisé en ce que le complément de signature s est établi à partir d'une fonction de hachage SHA(m, a) d'un message m à signer et de l'aléa *a*, et en ce que la même fonction de hachage est utilisée pour la vérification de signature.

12. Procédé selon l'une des revendications 7 à 11, caractérisé en ce que le complément de signature est établi par un calcul faisant intervenir un aléa (J) stocké dans la carte et ayant servi à établir le coupon de signature.

13. Procédé selon la revendication 12, caractérisé en ce que ce calcul faisant intervenir l'aléa (J) stocké dans la carte fait aussi intervenir une fonction de hachage SHA(x, J, i) portant au moins sur cet aléa (J) et sur un indice i représentant un numéro du coupon utilisé, cette même fonction de hachage SHA(x, J, i) ayant été précédemment utilisée au cours du calcul de chaîne binaire longue prévu dans le calcul du coupon correspondant.

14. Procédé selon l'une des revendications 7 à 13, caractérisé en ce que le complément de signature est établi par un calcul faisant intervenir une fonction de hachage du coupon, la même fonction de hachage du coupon étant utilisée pour la vérification de signature.

15. Procédé de génération de signatures numériques de messages par un dispositif signataire et de vérification de ces signatures par un dispositif

vérifieur, le dispositif signataire comportant des moyens de calcul, de communication et de rétention de données comprenant au moins une mémoire non volatile programmable électriquement, procédé selon lequel on prépare des données chiffrées constituant des coupons de signature r_i que l'on charge dans la mémoire non-volatile et que le dispositif signataire utilise pour signer des messages, principalement caractérisé en ce que :

- les coupons sont compressés par application d'une fonction de compression (H), dite encore fonction de hachage, par une autorité certifiée avant d'être chargés dans la mémoire,

et en ce qu'il comporte les échanges suivants :

- un message m est transmis et ce message doit être certifié par une signature;
- le signataire envoie un coupon r_i au vérifieur,
- le vérifieur envoie un nombre aléatoire a au signataire et déclenche un chronomètre,
- le signataire calcule la signature s du message et l'envoie au vérifieur,
- le vérifieur arrête le chronomètre et vérifie que la signature a été obtenue par le secret détenu dans la carte et le coupon r_i reçu; cette vérification est faite en vérifiant l'égalité suivante : $v = f(r_i, s, m) = r_i$
- le vérifieur accepte la signature si la condition de vérification $v = r_i$ est remplie et si le temps chronométré ne dépasse pas une durée prédéterminé impartie.

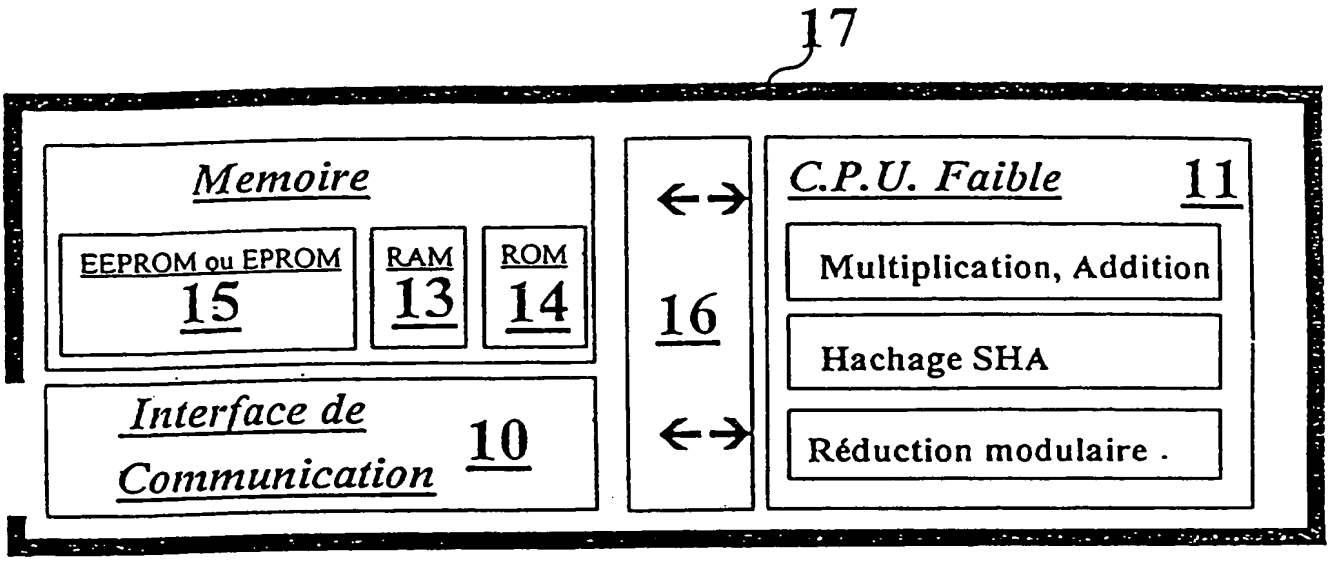

17
Memoire
EEPROM ou EPROM
15
RAM
13
ROM
14
Interface de Communication
10
16
C.P.U. Faible
11
Multiplication, Addition
Hachage SHA
Réduction modulaire .

FIG 1

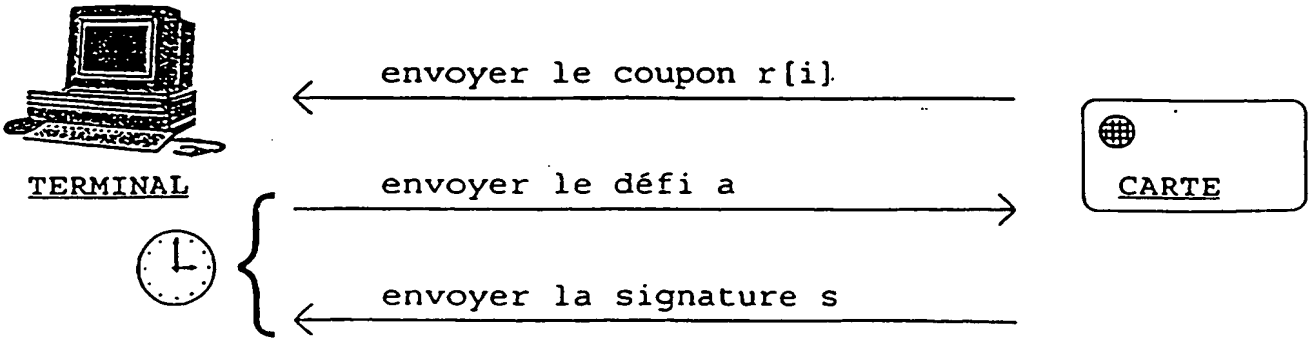

envoyer le coupon r[i]
TERMINAL
envoyer le défi a
CARTE
envoyer la signature s

FIG 2

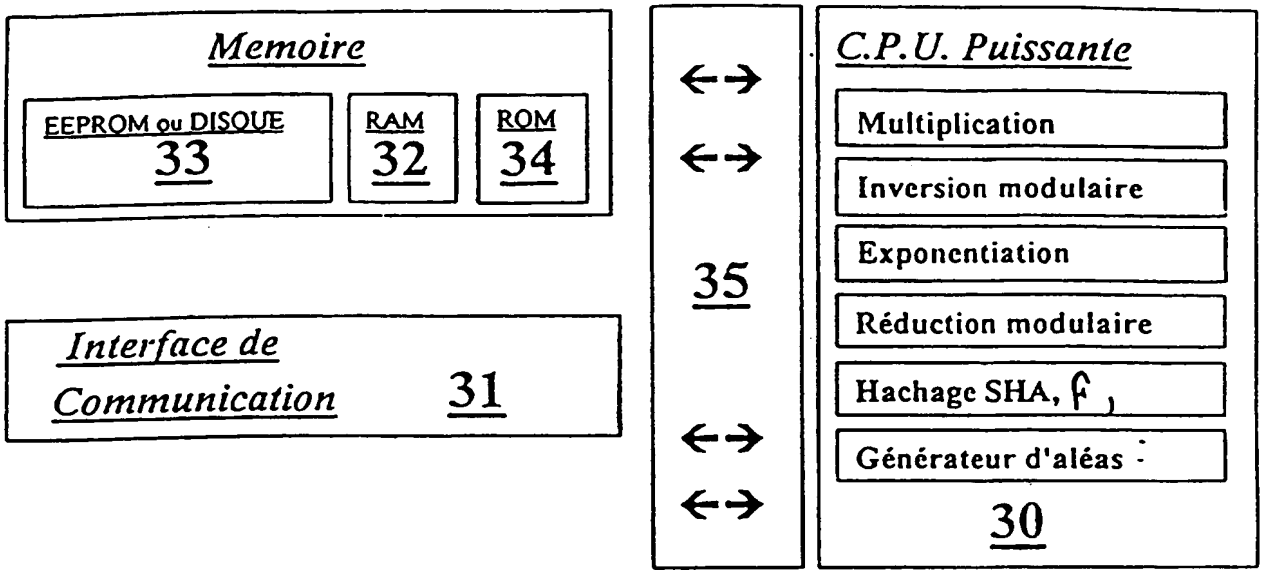

Memoire
EEPROM ou DISQUE
33
RAM
32
ROM
34
Interface de Communication
31
35
C.P.U. Puissante
Multiplication
Inversion modulaire
Exponentiation
Réduction modulaire
Hachage SHA, f
Générateur d'aléas
30

FIG 3

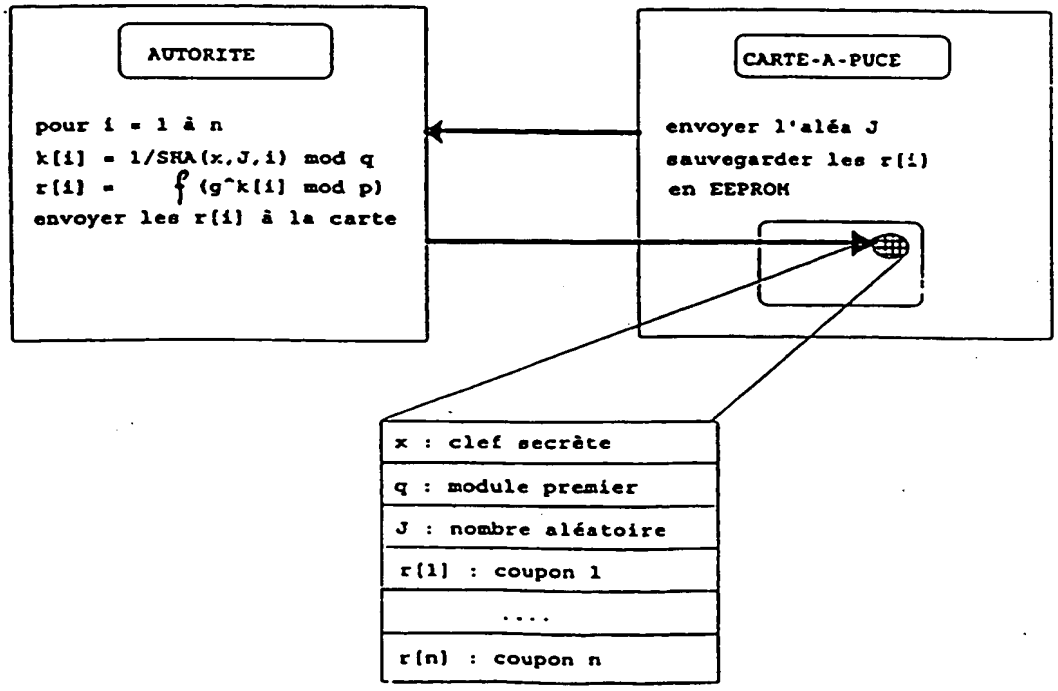

AUTORITE
pour i = 1 à n
k[i] = 1/SHA(x,J,i) mod q
r[i] = f(g^k[i] mod p)
envoyer les r[i] à la carte
CARTE-A-PUCE
envoyer l'aléa J
sauvegarder les r[i]
en EEPROM
x : clef secrète
q : module premier
J : nombre aléatoire
r[1] : coupon 1
....
r[n] : coupon n

FIG 4

INTERNATIONAL SEARCH REPORT

Intern ul Application No
PCT/FR 96/00612

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP,A,0 186 038 (CASIO) 2 July 1986 see page 2, line 9 - line 25 see page 3, line 7 - line 25 see page 4, line 4 - line 9 see page 8, line 21 - page 9, line 28 see page 12, line 9 - page 14, line 29 see page 15, line 36 - page 16, line 5 ---	1 15
A	BYTE, vol. 18, no. 12, November 1993, PETERBOROUGH (US), XP000408886 B. SCHNEIER: "DIGITAL SIGNATURES" see page 310, right-hand column, line 15 - page 311, left-hand column, line 11 see page 311, right-hand column, line 14 - line 50 --- -/--	2-4,7,15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

2

Date of the actual completion of the international search	Date of mailing of the international search report
16 July 1996	30. 07. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/FR 96/00612

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 4, no. 3, ISSN 0933-2790, pages 161-174, XP000573164 SCHNORR C P: "Efficient signature generation by smart cards" see page 172, line 6 - last line	2-4,7,15

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...rmation on patent family members

Interna... al Application No
PCT/FR 96/00612

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-186038	02-07-86	JP-C-	1825638	28-02-94
		JP-B-	5033416	19-05-93
		JP-A-	61139873	27-06-86
		CA-A-	1245764	29-11-88
		FR-A-	2574963	20-06-86
		US-A-	4710613	01-12-87

RAPPORT DE RECHERCHE INTERNATIONALE

Dem: Internationale No
PCT/FR 96/00612

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X A	EP,A,0 186 038 (CASIO) 2 Juillet 1986 voir page 2, ligne 9 - ligne 25 voir page 3, ligne 7 - ligne 25 voir page 4, ligne 4 - ligne 9 voir page 8, ligne 21 - page 9, ligne 28 voir page 12, ligne 9 - page 14, ligne 29 voir page 15, ligne 36 - page 16, ligne 5 ---	1 15
A	BYTE, vol. 18, no. 12, Novembre 1993, PETERBOROUGH (US), XP000408886 B. SCHNEIER: "DIGITAL SIGNATURES" voir page 310, colonne de droite, ligne 15 - page 311, colonne de gauche, ligne 11 voir page 311, colonne de droite, ligne 14 - ligne 50 --- -/--	2-4,7,15

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
16 Juillet 1996	30.07.96

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Holper, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demu Internationale No
PCT/FR 96/00612

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 4, no. 3, ISSN 0933-2790, pages 161-174, XP000573164 SCHNORR C P: "Efficient signature generation by smart cards" voir page 172, ligne 6 - dernière ligne	2-4,7,15

2

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux ...mbres de familles de brevets

Demande internationale No
PCT/FR 96/00612

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP-A-186038	02-07-86	JP-C-	1825638	28-02-94
		JP-B-	5033416	19-05-93
		JP-A-	61139873	27-06-86
		CA-A-	1245764	29-11-88
		FR-A-	2574963	20-06-86
		US-A-	4710613	01-12-87

TEXT AS FILED

Method for proving the authenticity of an entity and/or the integrity of a message by means of a public exponent equal to the power of two

The present invention relates to the methods, systems and devices designed to prove the authenticity of an entity and/or the integrity and/or authenticity of a message.

The patent EP 0 311 470 B1, whose inventors are Louis Guillou and Jean-Jacques Quisquater, describes such a method. Hereinafter, reference shall be made to their work by the terms "GQ patent" or "GQ method". Hereinafter, the expression "GQ2", or "GQ2 invention" or "GQ2 technology" shall be used to describe the present invention.

According to the GQ method, an entity known as a "trusted authority" assigns an identity to each entity called a "witness" and computes its RSA signature. In a customizing process, the trusted authority gives the witness an identity and signature. Thereafter, the witness declares the following: "Here is my identity; I know its RSA signature ". The witness proves that he knows the RSA signature of his identity without revealing this signature. Through the RSA public identification key distributed by the trusted authority, an entity known as a "controller" ascertains, without obtaining knowledge thereof, that the RSA signature corresponds to the declared identity. The mechanisms using the GQ method run "without transfer of knowledge". According to the GQ method, the witness does not know the RSA private key with which the trusted authority signs a large number of identities.

The GQ technology described here above makes use of RSA technology. However, while the RSA technology truly depends on the factorization of the modulus n, this dependence is not an equivalence, indeed far from it, as can be seen in what are called multiplicative attacks against various standards of digital signatures implementing the RSA technology.

The goal of the GQ2 technology is twofold: firstly to improve the performance characteristics of RSA technology and secondly to avert the problems inherent in RSA technology. Knowledge of the GQ2 private key is equivalent to knowledge of the factorization of the modulus n. Any attack on the triplets GQ2 leads to the

factorization of the modulus n: this time there is equivalence. With the GQ2 technology, the work load is reduced for the signing or self-authenticating entity and for the controller entity. Through a better use of the problem of factorizing in terms of both security and performance, the GQ2 technology averts the drawbacks of RSA technology.

The GQ method implements modulo computations of numbers comprising 512 bits or more. These computations relate to numbers having substantially the same size raised to powers of the order of $2^{16} + 1$. Now, existing microelectronic infrastructures, especially in the field of bank cards, make use of monolithic self-programmable microprocessors without arithmetical coprocessors. The work load related to multiple arithmetical applications involved in methods such as the GQ method leads to computation times which, in certain cases, prove to be disadvantageous for consumers using bank cards to pay for their purchases. It may be recalled here that, in seeking to increase the security of payment cards, the banking authorities have raised a problem that is particularly difficult to resolve. Indeed, two apparently contradictory questions have to be resolved: on the one hand, increasing security by using increasingly lengthy and distinct keys for each card while, on the other hand, preventing the work load from leading to excessive computation times for the user. This problem becomes especially acute inasmuch as it is also necessary to take account of the existing infrastructure and the existing microprocessor components.

The GQ2 technology provides a solution to this problem while boosting security.

Method

More particularly, the invention relates to a method designed to prove the following to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (**m** being greater than or equal to 1),

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),

- a public exponent **v**.

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \ . \ \mathbf{mod\ n} \text{ or } G_i \equiv Q_i^v \ \mathbf{mod\ n} \ .$$

Said exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$. The base number g_i is such that

the two equations:

$$x^2 \equiv g_i \ \mathbf{mod\ n} \quad \text{and} \quad x^2 \equiv -g_i \ \mathbf{mod\ n}$$

cannot be resolved in x in the ring of integers modulo **n** and such that:

the equation:

$$x^v \equiv g_i^2 \ \mathbf{mod\ n}$$

can be resolved in x in the ring of the integers modulo **n.**

Said method implements an entity called a witness in the following steps. Said witness entity has f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the $f.m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \ \mathbf{mod}\ p_j$) of the private values Q_i and of the public exponent **v**.

The witness computes commitments R in the ring of integers modulo **n**. Each commitment is computed:

- either by performing operations of the type:

$$R \equiv r^v \ \mathbf{mod\ n}$$

where r is a random value such that $0 < r < n$,

- or

- - by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

◦ ◦ then by applying the Chinese remainder method.

The witness receives one or more challenges **d**. Each challenge **d** comprises **m** integers d_i hereinafter called elementary challenges. The witness, on the basis of each challenge **d**, computes a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or

◦ ◦ by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method.

The method is such that there are as many responses $\mathbb{D}$ as there are challenges **d** as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, **d**, $\mathbb{D}$ forming a triplet referenced **{$\mathbb{R}$, d, $\mathbb{D}$}.**

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the method according to the invention is designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller. Said demonstrator entity comprises the witness. Said demonstrator and controller entities execute the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

At each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified here above. The demonstrator sends the controller all or part of each commitment $\mathbb{R}$.

◦ **Step 2: act of challenge d**

The controller, after having received all or part of each commitment $\mathbb{R}$, produces challenges **d** whose number is equal to the number of commitments $\mathbb{R}$ and sends the challenges **d** to the demonstrator.

◦ **Step 3: act of response $\mathbb{D}$**

The witness computes the responses **D** from the challenges **d** by applying the above-specified process.

- **Step 4: act of checking**

The demonstrator sends each response $\mathbb{D}$ to the controller.

First case: the demonstrator has transmitted a part of each commitment $\mathbb{R}$

If the demonstrator has transmitted a part of each commitment $\mathbb{R}$, the controller, having the **m** public values $G_1, G_2, ..., G_m$, computes a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

The controller ascertains that each reconstructed commitment $\mathbb{R}'$ reproduces all or part of each commitment $\mathbb{R}$ that has been transmitted to it.

Second case: the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

If the demonstrator has transmitted the totality of each commitment $\mathbb{R}$, the controller, having the **m** public values $G_1, G_2, ..., G_m$, ascertains that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

Case of the proof of the integrity of the message

In a second alternative embodiment capable of being combined with a first one, the method of the invention is designed to provide proof to an entity, known as the controller entity, of the integrity of a message $\mathbb{M}$ associated with an entity called a demonstrator entity. Said demonstrator entity comprises the witness. Said demonstrator and controller entities perform the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

At each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified here above.

◦ **Step 2: act of challenge d**

The demonstrator applies a hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$. The demonstrator sends the token $\mathbb{T}$ to the controller. The controller, after having received a token $\mathbb{T}$, produces challenges **d** equal in number to the number of commitments $\mathbb{R}$ and sends the challenges **d** to the demonstrator.

◦ **Step 3: act of response $\mathbb{D}$**

The witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the above-specified process.

◦ **Step 4: act of checking**

The demonstrator sends each response $\mathbb{D}$ to the controller. The controller, having the **m** public values $G_1, G_2, ..., G_m$, computes a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

Then the controller applies the hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$ to reconstruct the token $\mathbb{T}'$. Then the controller ascertains that the token $\mathbb{T}'$ is identical to the token $\mathbb{T}$ transmitted.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with the above two, the method according to the invention 1 is designed to produce the digital signature of a message $\mathbb{M}$ by an entity known as the signing entity. Said signing entity includes the witness.

Signing operation

Said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$.

Said signing entity executes the signing operation by implementing the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

At each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified here above. –

◦ **Step 2: act of challenge d**

The signing party applies a hashing function **h** whose arguments are the message $\mathbb{M}$ and each commitment $\mathbb{R}$ to obtain a binary train. From this binary train, the signing party extracts challenges **d** whose number is equal to the number of commitments $\mathbb{R}$.

◦ **Step 3: act of response $\mathbb{D}$**

The witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the above-specified process.

Checking operation

To prove the authenticity of the message $\mathbb{M}$, an entity called a controller checks the signed message. Said controller entity having the signed message carries out a checking operation by proceeding as follows.

◦ **Case where the controller has commitments $\mathbb{R}$, challenges d, responses $\mathbb{D}$**

If the controller has commitments $\mathbb{R}$, challenges **d**, responses $\mathbb{D}$, the controller ascertains that the commitments $\mathbb{R}$, the challenges **d** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

Then the controller ascertains that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d = h\ (\text{message}, R)$$

• Case where the controller has challenges d and responses D

If the controller has challenges **d** and responses **D**, the controller reconstructs, on the basis of each challenge **d** and each response **D**, commitments **R'** satisfying relationships of the type

$$R' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v/G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

Then the controller ascertains that the message **M** and the challenges **d** satisfy the hashing function:

$$d = h\ (\text{message}, R')$$

• Case where the controller has commitments R and responses D

If the controller has commitments **R** and responses **D**, the controller applies the hashing function and reconstructs **d'**

$$d' = h\ (\text{message}, R)$$

Then the controller device ascertains that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v/G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

System

The present invention also relates to a system designed to prove the following to a controller server:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$

(**m** being greater than or equal to 1),

- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),

- a public exponent **v**.

Said modulus, said exponent and said values are linked by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \text{ . mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n \text{ .}$$

Said exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of the base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$. The base number g_i is such that the two equations:

$$x^2 \equiv g_i \text{ mod } n \text{ and } x^2 \equiv - g_i \text{ mod } n$$

cannot be resolved in x in the ring of integers modulo **n** and such that the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n.**

Said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card. The witness device comprises a memory zone containing the **f** prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) of the private values Q_i and of the public exponent **v**. The witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device.

The computation means compute commitments **R** in the ring of integers modulo **n**. Each commitment is computed:

- either by performing operations of the type:

$$R \equiv r^v \text{ mod } n$$

where **r** is a random value produced by the random value production means, r being such that $0 < r < n$,

- or by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$, then by applying the Chinese remainder method.

The witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges.

- computation means, hereinafter called means for the computation of the responses $\mathbb{D}$ of the witness device for the computation, on the basis of each challenge **d, of** a response $\mathbb{D}$,

- either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

- or by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method.

The witness device also comprises transmission means to transmit one or more commitments $\mathbb{R}$ and one or more responses $\mathbb{D}$. There are as many responses $\mathbb{D}$ as there are challenges **d** as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, **d**, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the system according to the invention is designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

Said system is such that it comprises a demonstrator device associated with a demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic

microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said system also comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

Said system is used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

At each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified here above. The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means. The demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment $\mathbb{R}$ to the controller device through the connection means.

- **Step 2: act of challenge d**

The controller device comprises challenge production means for the production, after receiving all or part of each commitment $\mathbb{R}$, of the challenges **d** equal in number to the number of commitments $\mathbb{R}$. The controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

- **Step 3: act of response $\mathbb{D}$**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means. The means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified here above.

- **Step 4: act of checking**

The transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller. The controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device.

First case: the demonstrator has transmitted a part of each commitment $\mathbb{R}$.

If the transmission means of the demonstrator have transmitted a part of each commitment $\mathbb{R}$, the computation means of the controller device, having m public values $G_1, G_2, ..., G_m$, compute a reconstructed commitment $\mathbb{R}'$, from each challenge d and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

The comparison means of the controller device compare each reconstructed commitment $\mathbb{R}'$ with all or part of each commitment $\mathbb{R}$ received.

Second case: the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

If the transmission means of the demonstrator have transmitted the totality of each commitment $\mathbb{R}$, the computation means and the comparison means of the controller device, having m public values $G_1, G_2, ..., G_m$, ascertain that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the system according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity

known as a demonstrator. Said system is such that it comprises a demonstrator device associated with the demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. Said demonstrator device may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said system also comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

Said system is used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

At each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified here above. The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means.

- **Step 2: act of challenge d**

The demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function $\mathbb{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$. The demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token $\mathbb{T}$ through the connection means to the controller device. The controller device also has challenge production means for the production, after having received the token $\mathbb{T}$, of the challenges $\mathbf{d}$ in a number equal to the number of commitments $\mathbb{R}$. The controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges $\mathbf{d}$ to the demonstrator through the connection means.

- **Step 3: act of response $\mathbb{D}$**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means. The means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified here above.

- **Step 4: act of checking**

The transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller. The controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values G_1, G_2, ..., G_m, to firstly compute a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

then, secondly, compute a token $\mathbb{T}'$ by applying the hashing function **h** having as arguments the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$.

The controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token $\mathbb{T}'$ with the received token $\mathbb{T}$.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the system according to the invention is designed to prove the digital signature of a message $\mathbb{M}$, hereinafter known as a signed message, by an entity called a signing entity. The signed message comprises:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$.

Signing operation

Said system is such that it comprises a signing device associated with the signing entity. Said signing device is interconnected with the witness device by

interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said system is used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

At each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means.

- **Step 2: act of challenge d**

The signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function h whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute a binary train and extract, from this binary train, challenges $\mathbf{d}$ whose number is equal to the number of commitments $\mathbb{R}$.

- **Step 3: act of response $\mathbb{D}$**

The means for the reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the signing device through the interconnection means. The means for computing the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbf{d}$ by applying the process specified here above.

The witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbb{D}$ to the signing device through the interconnection means.

Checking operation

To prove the authenticity of the message $\mathbb{M}$, an entity known as the controller checks the signed message.

The system comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical,

electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device.

The signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means. Thus the controller device has a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

The controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

• Case where the controller device has commitments R, challenges d, responses D

Should the controller device have commitments **R**, challenges **d**, responses **D**, the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Then, the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d = h\,(\text{message}, R)$$

• Case where the controller device has challenges d and responses D

If the controller has challenges **d** and responses $\mathbb{D}$, the controller reconstructs, on the basis of each challenge **d** and each response $\mathbb{D}$, commitments $\mathbb{R}'$ satisfying relationships of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Then the controller ascertains that the message $\mathbb{M}$ and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, \mathbb{R}')}$$

- **Case where the controller has commitments $\mathbb{R}$ and responses $\mathbb{D}$**

If the controller has commitments $\mathbb{R}$ and responses $\mathbb{D}$, the computation means of the controller device apply the hashing function and compute **d'** such that

$$\mathbf{d' = h\ (message, \mathbb{R})}$$

Then the computation and comparison means of the controller device ascertain that the commitments $\mathbb{R}$, the challenges **d'** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Terminal Device

The invention also relates to a terminal device associated with an entity. The terminal device especially take the form of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. The terminal device is designed to prove the following to a controller server:

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$

(**m** being greater than or equal to 1),

- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),

- a public exponent **v**.

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \ . \ \mathbf{mod\ n} \text{ or } G_i \equiv Q_i^v \ \mathbf{mod\ n} \ .$$

Said exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of the base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$. The base number g_i is such that:

the two equations:

$$x^2 \equiv g_i \ \mathbf{mod\ n} \quad \text{and} \quad x^2 \equiv -g_i \ \mathbf{mod\ n}$$

cannot be resolved in x in the ring of integers modulo **n** and such that

the equation:

$$x^v \equiv g_i^2 \ \mathbf{mod\ n}$$

can be resolved in x in the ring of the integers modulo **n**.

Said terminal device comprises a witness device comprising a memory zone containing the **f** prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \ \mathbf{mod}\ p_j$) of the private values Q_i and of the public exponent **v**.

The witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments $\mathbb{R}$ of the witness device, to compute commitments $\mathbb{R}$ in the ring of the integers modulo **n**.

Each commitment is computed:

- either by performing operations of the type:

$$R \equiv r^{v} \bmod n$$

where r is a random value produced by the random value production means, r being such that $0 < r < n$,

- or by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$ produced by the random value production means, then by applying the Chinese remainder method.

The witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges.

- computation means, hereinafter called means for the computation of the responses $\mathbb{D}$ of the witness device, for the computation, on the basis of each challenge d, of a response $\mathbb{D}$,

- either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

- or by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method.

Said witness device also comprises transmission means to transmit one or more commitments $\mathbb{R}$ and one or more responses $\mathbb{D}$. There are as many responses $\mathbb{D}$ as there are challenges d as there are commitments $\mathbb{R}$. Each group of numbers $\mathbb{R}$, d, $\mathbb{D}$ forms a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the terminal device according to the invention is designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

Said terminal device is such that it comprises a demonstrator device associated with a demonstrator entity. Said demonstrator device is interconnected

with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said demonstrator device also comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

- **Step 1: act of commitment R**

At each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified here above.

The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means. The demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment $\mathbb{R}$ to the controller device, through the connection means.

- **Steps 2 and 3: act of challenge d, act of response $\mathbb{D}$**

The means of reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device. The means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbf{d}$ by applying the process specified here above.

- **Step 4: act of checking**

The transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller that carries out the check.

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the terminal device according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity known as a demonstrator. Said terminal device is such that it comprises a demonstrator device associated with the demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said demonstrator device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

At each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means.

- **Steps 2 and 3: act of challenge $\mathbf{d}$, act of response $\mathbb{D}$**

The demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function $\mathbb{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$. The demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token $\mathbb{T}$, through the connection means, to the controller device.

Said controller, after having received the token $\mathbb{T}$, produces challenges $\mathbf{d}$ in a number equal to the number of commitments $\mathbb{R}$

The means of reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the controller device through the connection means

between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device. The means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified here above.

◦ **Step 4: act of checking**

The transmission means of the demonstrator send each response $\mathbb{D}$ to the controller device which performs the check.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the terminal device according to the invention is designed to produce the digital signature of a message $\mathbb{M}$, hereinafter known as a signed message, by an entity called a signing entity. The signed message comprises:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$.

Said terminal device is such that it comprises a signing device associated with the signing entity. Said signing device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said demonstrator device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Signing operation

Said terminal device is used to execute the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

At each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission

means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the signing device through the interconnection means.

◦ **Step 2: act of challenge d**

The signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments $\mathbb{R}$.

◦ **Step 3: act of response $\mathbb{D}$**

The means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means. The means for computing the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified here above. The witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbb{D}$ to the signing device, through the interconnection means.

Controller Device

The invention also relates to a controller device. The controller device may especially take the form of a terminal or remote server associated with a controller entity. The controller device is designed to check:

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of public values $G_1, G_2, \ldots G_m$ (**m** being greater than or equal to 1),
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2), unknown to the controller device and to the associated controller entity,
- a public exponent **v**.

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \ . \ \mathbf{mod\ n} \text{ or } G_i \equiv Q_i^{-v} \mathbf{mod\ n} \ .$$

where Q_i designates a private value, unknown to the controller device, associated with the public value G_i.

The exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$. The base number g_i is such that

the two equations:

$$x^2 \equiv g_i \mathbf{mod\ n} \text{ and } x^2 \equiv -g_i \mathbf{mod\ n}$$

cannot be resolved in x in the ring of integers modulo **n** and such that:

the equation:

$$x^v \equiv g_i^2 \mathbf{mod\ n}$$

can be resolved in x in the ring of the integers modulo **n.**

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the controller device according to the invention is designed to prove the authenticity of an entity called a demonstrator and an entity called a controller.

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity.

Said controller device is used to execute the following steps:

- **Steps 1 and 2: act of commitment R, act of challenge d**

Said controller device also has means for the reception of all or part of the commitments R coming from the demonstrator device through the connection means.

The controller device has challenge production means for the production, after receiving all or part of each commitment R, of the challenges **d** in a number equal to the number of commitments R, each challenge **d** comprising **m** integers d_j hereinafter called elementary challenges.

The controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

◦ **Steps 3 and 4: act of response $\mathbb{D}$, act of checking**

The controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device.

First case: the demonstrator has transmitted a part of each commitment $\mathbb{R}$.

If the reception means of the demonstrator have received a part of each commitment $\mathbb{R}$, the computation means of the controller device, having **m** public values G_1, G_2, ..., G_m, compute a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

The comparison means of the controller device compare each reconstructed commitment $\mathbb{R}'$ with all or part of each commitment $\mathbb{R}$ received.

Second case: the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

If the transmission means of the demonstrator have transmitted the totality of each commitment $\mathbb{R}$, the computation means and the comparison means of the controller device, having **m** public values G_1, G_2, ..., G_m, ascertain that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$R \equiv D^{v}/G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, \mathrm{mod}\ n$$

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the controller device according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message M associated with an entity known as a demonstrator.

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity.

Said system is used to execute the following steps:

- **Steps 1 and 2: act of commitment R, act of challenge d**

Said controller device also has means for the reception of tokens T coming from the demonstrator device through the connection means. The controller device has challenge production means for the production, after having received the token T, of the challenges **d** in a number equal to the number of commitments R, each challenge **d** comprising **m** integers d_i, herein after called elementary challenges. The controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

- **Steps 3 and 4: act of response D, act of checking**

The controller device also comprises means for the reception of the responses D coming from the demonstrator device, through the connection means. Said controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, to firstly compute a reconstructed commitment R', from each challenge **d** and each response D, this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, D^{v} \ \mathrm{mod}\ n$$

or a relationship of the type

$$R' \equiv D^{v}/G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, \mathrm{mod}\ n$$

then, secondly, compute a token $\mathbb{T}'$ by applying the hashing function **h** having as arguments the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$.

The controller device also has comparison means, hereinafter called the comparison means of the controller device, to compare the computed token $\mathbb{T}'$ with the received token $\mathbb{T}$.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the controller device according to the invention is designed to prove the authenticity of the message $\mathbb{M}$ by checking a signed message by means of an entity called a controller.

The signed message, sent by a signing device associated with a signing entity having a hashing function **h (message, R)** comprises:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$.

Checking operation

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity. Said controller device receives the signed message from the signed device, through the connection means.

The controller device comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

◦ Case where the controller device has commitments $\mathbb{R}$, challenges d, responses $\mathbb{D}$

If the controller has commitments $\mathbb{R}$, challenges **d**, responses $\mathbb{D}$, the computation and comparison means of the controller device ascertain that the

commitments R, the challenges **d** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Then the computation and comparison means of the controller device ascertain that the message M, the challenges **d** and the commitments R satisfy the hashing function:

$$d' = h \text{ (message, } R)$$

- **Case where the controller device has challenges d and responses D**

If the controller device has challenges **d** and responses D, the computation means of the controller, on the basis of each challenge **d** and each response D, compute commitments R' satisfying relationships of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Then the computation and comparison means of the controller device ascertain that the message M and the challenges **d** satisfy the hashing function:

$$d = h \text{ (message, } R')$$

- **Case where the controller device has commitments R and responses D**

If the controller device has commitments R and responses D, the computation means of the controller device apply the hashing function and compute **d'** such that

$$d = h \text{ (message, } R)$$

Then the computation and comparison means of the controller device ascertain that the commitments R, the challenges **d'** and the responses D satisfy relationships of the type

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v/G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

Description

The goal of GQ technology may be recalled: it is the dynamic authentication of entities and associated messages as well as the digital signature of messages.

The standard version of GQ technology makes use of RSA technology. However, although the RSA technology truly depends on factorizing, this dependence is not an equivalence, far from it, as can be shown from attacks, known as multiplicative attacks, against various digital signature standards implementing RSA technology.

In the context of GQ2 technology, the present part of the invention relates more specifically to the use of sets of GQ2 keys in the context of dynamic authentication and digital signature. The GQ2 technology does not use RSA technology. The goal is a twofold one: first to improve performance with respect to RSA technology and secondly to prevent problems inherent in RSA technology. The GQ2 private key is the factorization of the modulus n. Any attack on the GQ2 triplets amounts to the factorizing of the modulus n: this time there is equivalence. With the GQ2 technology, the work load is reduced both for the entity that signs or is authenticated and for the one that checks. Through an improved use of the problem of factorization, in terms of both security and performance, the GQ2 technology rivals the RSA technology.

The GQ2 technology uses one or more small integers greater than 1, for example m small integers ($m \geq 1$) called base numbers and referenced g_i. Since the base numbers are fixed from g_i to g_m with $m > 1$, a public verification key $\langle v, n \rangle$ is chosen as follows. The public verification exponent v is 2^k where k is a small integer greater than 1 ($k \geq 2$). The public modulus n is the product of at least two prime factors greater than the base numbers, for example f prime factors ($f \geq 2$) referenced by p_j, from $p_1 \ldots p_f$. The f prime factors are chosen so that the public modulus n has the following properties with respect to each of the m base numbers from g_1 to g_m.

- Firstly, the equations (1) and (2) cannot be resolved in x in the ring of the integers modulo n, that is to say that g_i and $-g_i$ are two non-quadratic residues (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$

$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- Secondly, the equation (3) can be resolved in x in the ring of the integers modulo n.

$$x^{2^k} \equiv g_i^2 \pmod{n} \qquad (3)$$

Since the public verification key $\langle v, n \rangle$ is fixed according to the base numbers from g_1 to g_m with $m \geq 1$, each base number g_i determines a pair of values GQ2 comprising a public value G_i and a private value Q_i: giving m pairs referenced G_1 Q_1 to G_m Q_m. The public value G_i is the square of the base number g_i: giving $G_i = g_i^2$. The private value Q_i is one of the solutions to the equation (3) or else the inverse (mod n) of such a solution.

Just as the modulus n is broken down into f prime factors, the ring of the integers modulo n are broken down into f Galois fields, from CG(p_1) to CG(p_f). Here are the projections of the equations (1), (2) and (3) in CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Each private value Q_i can be represented uniquely by f private components, one per prime factor: $Q_{i,j} \equiv Q_i \pmod{p_j}$. Each private component $Q_{i,j}$ is a solution to the equation (3.a) or else the inverse (mod p_j) of such a solution. After all the possible solutions to each equation (3.a) have been computed, the Chinese remainder technique sets up all the possible values for each private value Q_i on the basis of f components of $Q_{i,1}$ to $Q_{i,f}$: Q_i = Chinese remainders ($Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$) so as to obtain all the possible solutions to the equation (3).

The following is the Chinese remainder technique: let there be two positive integers that are mutually prime numbers a and b such that $0 < a < b$, and two components X_a from 0 to $a-1$ and X_b from 0 to $b-1$. It is required to determine X = Chinese remainders (X_a, X_b), namely the unique number X from 0 to $a.b-1$ such that $X_a \equiv X \pmod{a}$ and $X_b \equiv X \pmod{b}$. The following is the Chinese remainder parameter: $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. The following is the Chinese remainder

operation: $\varepsilon \equiv X_b \pmod a$; $\delta = X_a - \varepsilon$; if δ is negative, replace δ by $\delta + a$; $\gamma \equiv \alpha \,.\, \delta \pmod a$; $X = \gamma \,.\, b + X_b$.

When the prime factors are arranged in rising order, from the smallest p_1 to the greater p_f, the Chinese remainder parameters can be the following (there are $f-1$ of them, namely one less than prime factors). The first Chinese remainder parameter is $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. The second Chinese remainder parameter is $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. The i–th Chinese remainder parameter is $\lambda \equiv \{p_1.p_2. \ldots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. And so on and so forth. Finally, in $f-1$ Chinese remainder operations, a first result (mod p_2 times p_1) is obtained with the first parameter and then a second result (mod $p_1.p_2$ times p_3) with the second parameter and so on and so forth until a result (mod $p_1. \ldots p_{f-1}$ times p_f), namely (mod n).

There are several possible depictions of the private key GQ2, which expresses **the polymorphic nature of the private key GQ2**. The various depictions prove to be equivalent: they all amount to knowledge of the factorization of the module n which is the true private GQ2 key. If the depiction truly affects the behavior of the signing entity or self-authenticating entity, it does not affect the behavior of the controller entity.

Here are the main three possible depictions of the GQ2 private key.

1) The standard representation in GQ technology consists of the storage of m private values Q_i and the public verification key $<v, n>$; in GQ2, this depiction is rivalled by the following two. 2) The optimal representation in terms of work load consists in storing the public exponent v, the f prime factors p_j, $m.f$ private components Q_{ij} and f-1 parameters of the Chinese remainders. 3) The optimal representation in terms of private key size consists in storing the public exponent v, the m basic numbers g_i and the f prime factors p_j, then in starting each use by setting up either m private values Q_i and the module n to return to the first depiction or else $m.f$ private components $Q_{i,j}$ and f-1 parameters of the Chinese remainders to return to the second one.

The signing or self-authenticating entities can all use the same base numbers. Unless otherwise indicated, the m base numbers from g_1 to g_m can then advantageously be the m first prime numbers;

Because the security of the dynamic authentication mechanism or digital signature mechanism is equivalent to knowledge of a breakdown of the modulus, the GQ2 technology cannot be used to simply distinguish two entities using the same modulus. Generally, each entity that authenticates itself or signs has its own GQ2 modulus. However, it is possible to specify GQ2 moduli with four prime factors, two of which are known by an entity and the other two by another entity.

Here is a first set of GQ2 keys with $k = 6$, giving $v = 64$, $m = 3$, giving three base: $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, and $f = 3$, namely a modulus with three prime factors: two congruent to 3 (mod 4) and one to 5 (mod 8). It must be noted that $g = 2$ is incompatible with a prime factor congruent to 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9CO5A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4DA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A

C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4
DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8
82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A
AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197
697238537FE7A0195C5E8373EB74D

The following is a second set of GQ2 keys, with $k = 9$, that is $v = 512$, $m = 2$, that is two base numbers: $g_1 = 2$ and $g_2 = 3$, and $f = 3$, giving a modulus with three prime factors congruent to 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D
6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49
761B276A8E6B6977A21D5i669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = O45ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C
35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6
EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64

9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Dynamic authentication

The dynamic authentication mechanism is designed to prove, to an entity known as a **controller**, the authenticity of another entity known as a **demonstrator** as well as the authenticity of a possible associated message *M*, so that the controller can be sure that it is truly the demonstrator and, as the case may be, only the demonstrator and that the demonstrator is truly speaking of the same message *M*. The associated message *M* is optional. This means that it may be vacant.

The dynamic authentication mechanism is a sequence of four acts: an act of commitment, and act of challenge, and act of response and an act of checking. The demonstrator fulfills the acts of commitment and response. The controller fulfills the acts of challenge and control.

Within the demonstrator, it is possible to isolate a witness so as to isolate the most sensitive parameters and functions of the demonstrator, namely the production of commitments and responses. The witness has the parameter *k* and the private key GQ2, namely the factorization of the module *n* according to one of the three depictions referred to here above: ∘ the *f* prime factors and the *m* base numbers, ∘ the *m.f* private component, the *f* prime factors and the *f*-1 parameters of the Chinese remainders, ∘ the *m* private values and the modulus *n*.

The witness may correspond to a partial embodiment, for example, ∝ a chip card connected to a PC forming the entire demonstrator or again, ∝ specially protected programs within a PC, or again, ∘ specially protected programs within a smart card. The witness thus isolated is similar to the witness defined here below within the signing party. At each execution of the mechanism, the witness produces one or more commitments *R* and then as many responses *D* to as many challenges *d*. Each set {*R, d, D*} is a **GQ2 triplet**.

Apart from comprising the witness, the demonstrator also has, if necessary, a hashing function and a message *M*.

The controller has the modulus n and the parameters k and m; if necessary, it also has the same hashing function and a message M'. The controller is capable of reconstituting a commitment R' from any challenge d and any response D. The parameters k and m inform the controller. Failing any indication to the contrary, the m base numbers from g_1 to g_m are the m first prime numbers. Each challenge d must have m elementary challenges referenced from d_1 to d_m: one per base number. This elementary challenge from d_1 to d_m may take a value of 0 to $2^{k-1}-1$ (the values of $v/2$ to v-1 are not used). Typically, each challenge is encoded by m times k-1 bits (and not by m times k bits). For example, $k = 6$ and $m = 3$ and the base numbers 3, 5 and 7, each challenge has 15 bits transmitted on two bytes; with $k = 9$, $m = 2$ and the base numbers 2 and 3, each challenge has 16 bits transmitted on two bytes. When the $(k\text{-}1).m$ possible challenges are also possible, the value $(k\text{-}1).m$ determines the security provided by each GQ2 triplet: an impostor who, by definition, does not know the factorization of the module n has exactly one chance of success in $2^{(k-1).m}$. When $(k\text{-}1).m$ is equal to 15 to 20, one triplet is enough to reasonably provide for dynamic authentication. To achieve any security level, it is possible to produce triplets in parallel. It is also possible to produce sequentially, namely to repeat the execution of the mechanism.

1) **The act of commitment** comprises the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n, it draws one or more random values r ($0 < r < n$) at random and privately; then by k successive squaring (mod n) operations, it converts each random value r into a commitment R.

$$R \equiv r^v \pmod{n}$$

Here is an example with the first set of keys with $k = 6$.

r = B8AD426C1A10165E94B894AC2437C1B1797EF562CFA53A4AF8
43131FF1C89CFDA131207194710EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

R = FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56
D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04

49CC4292E5DD2BDB00828AF18

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij}, it draws one or more collections of f random values at random and privately: each collection has one random value r_i per prime factor p_i ($0 < r_i < p_i$); then by k successive operations of squaring (mod p_i), it converts each random value r_i into a component of commitment R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Here is an example with the second set of keys with $k = 9$.

r_1 = B0418EABEBADF0553A28903F74472CD49DD8C82D86

R_1 = 022B365F0BEA8E157E94A9DEB0512827FFD5149880F1

r_2 = 75A8DA8FE0E60BD55D28A218E31347732339F1D667

R_2 = 057^{E}43A242C455FC20DEEF291C774CF1B30F0163DEC2

r_3 = 0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27

R_3 = 06^{E}14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C

For each collection of f commitment components, the witness sets up a commitment according to the technique of Chinese remainders. There are as many commitments as there are collections of random values.

$$R = \text{Chinese remainders } (R_1, R_2, ..., R_j)$$

R = 28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7

D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9

9123B56446F6C928736B17B4BA4A529

In both cases, the demonstrator sends the controller all or part of each commitment R, or at least a hashing code H obtained by hashing each commitment R and one message M.

2) The act of challenge consists in drawing at random one or more challenges d each consisting of m elementary challenges $d_1 \,/\, d_2 \,/\, \ldots \,/\, d_m$; each elementary challenge d_i takes one of the values from 0 to v/2-1.

$$d = d_1 \,/\, d_2 \,/\, \ldots \,/\, d_m$$

Here is an example for the first set of keys with $k = 6$ and $m = 3$.

$d_1 = 10110 = 22 = $ '16'; $d_2 = 00111 = 7$; $d_3 = 00010 = 2$

$d = 0 \,||\, d_1 \,||\, d_2 \,||\, d_3 = 01011000\ 11100010 = 58\ E2$

Here is an example for the second set of keys with $k = 9$ and $m = 2$.

$d = d_1 \,||\, d_2$ = 58 E2, that is, in decimal notation 88 and 226

The controller sends the demonstrator each challenge ***d***.

3) The act of response has the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n, it computes one or more responses D in using each random value r of the act of commitment and the private values according to the elementary challenges.

$$X \equiv Q_1^{d1}.Q_2^{d2}...Q_m^{dm} (\text{mod } n)$$

$$D \equiv r.X \text{ (mod n)}$$

Here is an example for the first set of keys.

D = FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386
5EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480
A2C6A290273479FEC9171990A17

When the witness has f prime factors from p_i to p_f and $m.f$ private components $Q_{i,j}$, it computes one or more collections of f response components in using each collection of random values of the act of commitment: each collection of response components comprises one component per prime factor.

$$X_i \equiv Q_1^{d1}.Q_2^{d2}...Q_m^{dm},_i (\text{mod } p_i)$$

$$D_i \equiv r_i.X_i (\text{mod } p_1)$$

Here is an example for the second set of keys.

$D_1 = r_1.\ Q_{1.1}^{d1}.Q_{2.1}^{d2} (\text{mod } p_1) =$
O2660ADF3C73B6DC15E196152322DDE8EB5B35775E38

$D_2 = r_2.\ Q_{1.2}^{d1}.Q_{2.2}^{d2} (\text{mod } p_2) =$
04C15028E5FD1175724376C11BE77052205F7C62AE3B

$D_3 = r_3.\ Q_{1.3}^{d1}.Q_{2.3}^{d2} (\text{mod } p_3) =$
0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52

For each collection of response components, the witness draws up a response according to the Chinese remainder technique. There are as many responses as there are challenges.

D = Chinese reminders (D_1, D_2, ..., D_f)

D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36
4CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00
195A7305C6FF3323F72DC1AB

In both cases, the demonstrator sends each response ***D*** to the controller.

4) The checking act consists in ascertaining that each triplet $\{R, d, D\}$ verifies an equation of the following type for a non-zero value,

$$R\cdot\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \text{ or else } R \equiv D^{2^k}\cdot\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

or else in setting up each commitment: none should be zero.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \text{ or else } R' \equiv D^{2^k}\cdot\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

If necessary, the controller then computes a hashing code H' in hashing each re-established commitment R' and a message M'. The dynamic authentication is successful when the controller thus retrieves what it had received at the end of the first act of commitment, namely all or part of each commitment R, or else the hashing code H.

For example, a sequence of elementary operations converts the response D into a commitment R'. The sequence has k squares (mod n) separated by k-1 divisions or multiplications (mod n) by base numbers. For the i-th division or multiplication, which is performed between the i-th square and the i+1st square, the i-th bit of the elementary challenge d_i indicates that it is necessary to use g_i, the i-th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2, ... up to the i-th bit of the elementary challenge d_m which indicates that it is necessary to use g_m.

Here is an example for the first set of keys.

$D^2 \pmod{n}$ = FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733

3 . $D^2 \pmod{n}$ = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF

$3^2 \cdot D^4 \pmod{n}$ = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

$3^4 \cdot D^8 \pmod{n}$ = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

$3^5 \cdot 5 \cdot D^8 \pmod{n}$ = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

$3^{10} \cdot 5^2 \cdot D^{16} \pmod{n}$ = BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD
B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} \cdot 5^3 \cdot 7 \cdot D^{16} \pmod{n}$ = DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} \cdot 5^6 \cdot 7^2 \cdot D^{32} \pmod{n}$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} \cdot 5^7 \cdot 7^2 \cdot D^{32} \pmod{n}$ = DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} \cdot 5^{14} \cdot 7^4 \cdot D^{64} \pmod{n}$, namely $3^{2C} \cdot 5^E \cdot 7^4 \cdot D^{40}$ with the exponents in hexadecimal notation = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

We find the commitment R. The authentication is successful.

Here is an example for the second set of keys.

$D^2 \pmod{n}$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

$3 \cdot D^2 \pmod n$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^2 \cdot D^4 \pmod n$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 \cdot 3^3 \cdot D^4 \pmod n$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5

$2^2 \cdot 3^6 \cdot D^5 \pmod n$ = 4C210F96FF6C77541910623B1E49533206DFB9E91
6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8

$2^2 \cdot 3^7 \cdot D^8 \pmod n$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388

$2^4 \cdot 3^{14} \cdot D^{16} \pmod n$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^5 \cdot 3^{14} \cdot D^{16} \pmod n$ = DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} \cdot 3^{28} \cdot D^{32} \pmod n$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} \cdot 3^{28} \cdot D^{32} \pmod n$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} \cdot 3^{56} \cdot D^{64} \pmod n$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

$2^{44} \cdot 3^{112} \cdot D^{128} \pmod n$ = 925B0EDF5047EFEC5AFABDC03A830919761

B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F
8FDEC740778BDC178AD7AF2968689B930D5A2359

$2^{44} \cdot 3^{153} \cdot D^{128} \pmod{n}$ = B711D89C03FDEA8D1F889134A4F809B3F2D
8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803
BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} \cdot 3^{226} \cdot D^{256} \pmod{n}$ = 41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C
08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D
FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} \cdot 3^{452} \cdot D^{512} \pmod{n}$ that is $4^{88} \cdot 9^{226} \cdot D^{512} \pmod{n}$ = 28AA7F12259BFBA8
1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D
AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA
4A529

We find the commitment R. The authentication is successful.

Digital signature

The digital signing mechanism enables an entity called a **signing party** to produce signed messages and an entity called a **controller** to ascertain signed messages. The message M is any binary sequence: it may be vacant. The message M is signed by adding a signature appendix to it. This signature appendix comprises one or more commitments and/or challenges as well as the corresponding responses.

The controller has the same hashing function, the parameters k and m and the module n. The parameters k and m provide information to the controller. Firstly, each elementary challenge from d_1 to d_m must take a value from 0 to 2_{k-1}-1 (the values of $v/2$ to v-1 are not used). Secondly, each challenge d must comprise m elementary challenges referenced from d_1 to d_m, namely as many of them as base numbers. Furthermore, failing indications to the contrary, the m base numbers from g_1 to g_m are the m first prime numbers. With $(k\text{-}1).m$ equal to 15 to 20, it is possible to sign with four triplets GQ2 produced in parallel; with $(k\text{-}1).m$ equal to 60 or more, it is possible to sign with a single triplet GQ2. For example, with $k = 9$ and $m = 8$, a single triplet GQ2 is enough; each challenge has eight bytes and the base numbers are 2, 3, 5, 7, 11, 13, 17 and 19.

The signing operation is a sequence of three acts: an act of commitment, an act of challenge and an act of response. Each act produces one or more GQ2 triplets each comprising: a commitment R ($\neq 0$), a challenge d consisting of m elementary challenges referenced $d_1, d_2, ..., d_m$ and a response D ($\neq 0$).

The signing party has a hashing function, the parameter k and the GQ2 private key, namely the factorization of the modulus n according to one of the three depictions referred to here above. **Within the signing party, it is possible to isolate a witness that performs the the acts of commitment and response**, so as to isolate the functions and parameters most sensitive to the demonstrator. To compute commitments and responses, the witness has the parameter k and the GQ2 private key, namely the factorization of the modulus n according to one of the three depictions referred to here above. The witness thus isolated is similar to the witness defined within the demonstrator. It may correspond to a particular embodiment, for example, ∝ a chip card connected to a PC forming the entire signing party, or again, ∝ programs particularly protected within a PC, or again, ∝ programs particularly protected within a chip card.

1) The act of commitment comprises the following operations:

When the witness has m private values from Q_1 to Q_m and the modulus n, it randomly and privately draws one or more random values r ($0 < r < n$); then, by k successful squaring (mod n) operations, it converts each random value r into a commitment R.

$$R_i \equiv r^v \pmod{n}$$

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij}, it privately and randomly draws one or more collections of f random values: each collection has one random value r_i per prime factor p_i ($0 < r_i < p_i$); then, by k successive squaring (mod p_i) operations, it converts each random value r_i into a component of commitment R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

For each collection of f commitment components, the witness sets up a commitment according to the Chinese remainder technique. There are as many commitments as there are collections of random values.

$$R = \text{Chinese remainders } (R_1, R_2, ..., R_f)$$

2) The act of challenge consists in hashing all the commitments R and the message to be signed M to obtain a hashing code from which the signing party forms one or more challenges each comprising m elementary challenges; each elementary challenge takes a value from 0 to $v/2$-1; for example with $k = 9$ and $m = 8$. Each challenge has eight bytes. There are as many challenges as there are commitments.

$$d = d_1 \,/\, d_2 \,/\, \ldots \,/\, d_m, \text{ extracted from the result Hash}(M, R)$$

3) The act of response comprises the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n, it computes one or more responses D using each random value r of the act of commitment and the private values according to the elementary challenges.

$$X. / \equiv Q_1^{d1}.Q_2^{d2}\ldots Q_m^{dm} \text{ (mod n)}$$

$$D / \equiv r. /X. / \text{ (mod n)}$$

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij}, it computes one or more collections of f response components in using each collection of random values of the act of commitment : each collection of response components comprises one component per prime factor.

$$X_i \equiv Q_1^{d1},_i \cdot Q_2^{d2},_i \ldots Q_m^{dm},_i \text{ (mod } p_i)$$

$$D_i \equiv r_i.X_i \text{ (mod } p_i)$$

For each collection of response components, the witness sets up a response according to the Chinese remainders technique. There are as many responses as there are challenges.

$$D = \text{Chinese remainders } (D_1, D_2, ..., D_f)$$

The signing party signs the message M in adding to it a signature appendix comprising:

- either each GQ2 triplet, namely each commitment R, each challenge d and each response D,

- or else each commitment R and each corresponding response D,

- or else each challenge d and each corresponding response D.

The running of the verification operation depends on the contents of the signature appendix. There are three possible cases.

Should the appendix comprise one or more triplets, the checking operation has two independent processes for which the chronology is not important. The controller accepts the signed message if and only if the two following conditions are fulfilled.

Firstly, each triplet must be consistent (an appropriate relationship for the following type has to be verified) and acceptable (the comparison has to be done on a non-zero value).

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^t} \pmod{n} \text{ or else } R \equiv D^{2^t}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

For example, the response D is converted by a sequence of elementary operations: k squared (mod n) separated by k-1 multiplication or division operations (mod n) by base numbers. For the i-th multiplication or division which is performed between the i-th square and the i+1st square, the i-th bit of the elementary challenge d_1 indicates whether it is necessary to use g_1, the i-th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2, ... up to the i-th bit of the elementary challenge d_m which indicates if it is necessary to use g_m. It is thus necessary to retrieve each commitment R present in the signature appendix.

Furthermore, the triplet or triplets must be linked to the message M. By hashing all the commitments R and the message M, a hashing code is obtained from which each challenge d must be recovered.

$d = d_1 \,/\, d_2 \,/\, \ldots \,/ d_m$, identical to those extracted from the result Hash(M, R)

Should the appendix have no challenge, the checking operation starts with a reconstruction of one or more challenges d' by hashing all the commitments R and the message M.

$D' = d'_1 \,/\, d'_2 \,/\, \ldots \,/\, d'_m$, extracted from the result Hash(M, R)

Then, the controller accepts the signed message if and only if each triplet is consistent (an appropriate relationship of the following type is verified) and acceptable (the comparison is done on a non-zero value).

$$R\cdot\prod_{i=1}^{m} G_i^{d'_i} \equiv D^{2^t} \pmod{n} \text{ or else } R\equiv D^{2^t}\cdot\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Should the appendix comprise no commitment, the checking operation starts by reconstructing one or more commitments R' according to one of the following two formulae, namely the one that is appropriate. No re-established commitment should be zero.

$$R'\equiv D^{2^t}/\prod_{i=1}^{m} G_i^{d_i} \pmod{n} \text{ or else } R'\equiv D^{2^t}\cdot\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Then, the controller must hash all the commitments R' and the message M so as to reconstitute each challenge d.

$d = d_1 \,/\, d_2 \,/\, \ldots \,/\, d_m$, identical to those extracted from the result Hash(M, R)

The controller accepts the signed message if and only if each reconstituted challenge is identical to the corresponding challenge in the appendix.

In the present application, it has been shown that there are pairs of private values and public values Q and G respectively used to implement the method, system and device according to the invention, designed to prove the authenticity of an entity and/or integrity and/or authenticity of a message.

In the pending application filed on the same day as the present application by France Télécom, TDF and the firm Math RiZK, whose inventors are Louis Guillou and Jean-Jacques Quisquater, a method has been described for the production of sets of GQ2 keys namely moduli n and pairs of public and private values G and Q respectively when the exponent v is equal to 2^k. This patent application is incorporated herein by reference.

CLAIMS

1. Method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (m being greater than or equal to 1),
- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$ (f being greater than or equal to 2),
- a public exponent v;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

said exponent v being such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo n

and such that:

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the $f.m$

components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments $\mathbb{R}$ in the ring of integers modulo n; each commitment being computed:

◦ either by performing operations of the type:

$$\mathbb{R} \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

◦ or

◦ ◦ by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

◦ ◦ then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or

◦ ◦ by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

◦ ◦ and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbb{D}$ as there are challenges d as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, d, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

2. Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment $\mathbb{R}$**

- at each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

- the demonstrator sending the controller all or part of each commitment $\mathbb{R}$,

◦ **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment $\mathbb{R}$, produces challenges **d** whose number is equal to the number of commitments $\mathbb{R}$ and sends the challenges **d** to the demonstrator,

◦ **Step 3: act of response $\mathbb{D}$**

- the witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the process specified in claim 1,

◦ **Step 4: act of checking**

- the demonstrator sends each response $\mathbb{D}$ to the controller,

case where the demonstrator has transmitted a part of each commitment $\mathbb{R}$

if the demonstrator has transmitted a part of each commitment $\mathbb{R}$, the controller, having the **m** public values $G_1, G_2, ..., G_m$, computes a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v/G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

the controller ascertains that each reconstructed commitment $\mathbb{R}'$ reproduces all or part of each commitment $\mathbb{R}$ that has been transmitted to it.

Case where the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

if the demonstrator has transmitted the totality of each commitment $\mathbb{R}$, the controller, having the **m** public values $G_1, G_2, ..., G_m$, ascertains that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v/G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

3. Method according to claim 1, designed to provide proof to an entity, known as the controller entity, of the integrity of a message $\mathbb{M}$ associated with an entity called a demonstrator entity, said demonstrator entity comprising the witness; said demonstrator and controller entities executing the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

- at each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

◦ **Step 2: act of challenge d**

- the demonstrator applies a hashing function $\mathbb{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$,
- the demonstrator sends the token $\mathbb{T}$ to the controller,
- the controller, after having received a token $\mathbb{T}$, produces challenges **d** equal in number to the number of commitments $\mathbb{R}$ and sends the challenges **d** to the demonstrator,

◦ **Step 3: act of response $\mathbb{D}$**

- the witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

◦ **Step 4: act of checking**

- the demonstrator sends each response $\mathbb{D}$ to the controller,
- the controller, having the $\mathbb{m}$ public values G_1, G_2, ..., G_m, computes a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

- then the controller applies the hashing function $\mathbb{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$ to reconstruct the token $\mathbb{T}'$,
- then the controller ascertains that the token $\mathbb{T}'$ is identical to the token $\mathbb{T}$ transmitted.

4. Method according to claim 1, designed to produce the digital signature of a message $\mathbb{M}$ by an entity known as the signing entity, said signing entity comprising the witness;

Signing operation

said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

said signing entity executes the signing operation by implementing the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

- at each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

◦ **Step 2: act of challenge d**

- the signing party applies a hashing function **h** whose arguments are the message $\mathbb{M}$ and each commitment $\mathbb{R}$ to obtain a binary train,
- from this binary train, the signing party extracts challenges **d** whose number is equal to the number of commitments $\mathbb{R}$,

◦ **Step 3: act of response $\mathbb{D}$**

- the witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1.

5. Method according to claim 4, designed to prove the authenticity of the message M by checking the signed message through an entity called a controller;

Checking operation

- said controller entity having the signed message executes a checking operation by proceeding as follows:

◦ **case where the controller has commitments $\mathbb{R}$, challenges d, responses $\mathbb{D}$**

if the controller has commitments $\mathbb{R}$, challenges **d**, responses $\mathbb{D}$,

∘ ∘ the controller ascertains that the commitments $\mathbb{R}$, the challenges $\mathbf{d}$ and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

∘ ∘ the controller ascertains that the message $\mathbb{M}$, the challenges $\mathbf{d}$ and the commitments $\mathbb{R}$ satisfy the hashing function:

$$\mathbf{d} = h\,(\text{message}, \mathbb{R})$$

∘ case where the controller has challenges $\mathbf{d}$ and responses $\mathbb{D}$

if the controller has challenges $\mathbf{d}$ and responses $\mathbb{D}$,

∘ ∘ the controller reconstructs, on the basis of each challenge $\mathbf{d}$ and each response $\mathbb{D}$, commitments $\mathbb{R}'$ satisfying relationships of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

∘ ∘ the controller ascertains that the message $\mathbb{M}$ and the challenges $\mathbf{d}$ satisfy the hashing function:

$$\mathbf{d} = h\,(\text{message}, \mathbb{R}')$$

∘ case where the controller has commitments $\mathbb{R}$ and responses $\mathbb{D}$

if the controller has commitments $\mathbb{R}$ and responses $\mathbb{D}$,

∘ ∘ the controller applies the hashing function and reconstructs $\mathbf{d}'$

$$\mathbf{d}' = h\,(\text{message}, \mathbb{R})$$

∘ ∘ the controller device ascertains that the commitments $\mathbb{R}$, the challenges $\mathbf{d}'$ and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

6. A system designed to prove, to a controller server,

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (m being greater than or equal to 1),

- a public modulus n constituted by the product of said f prime factors $p_1, p_2, \ldots p_f$ (f being greater than or equal to 2),

- a public exponent v.

said modulus, said exponent and said values being linked by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ or } G_i \equiv Q_i^{-v} \mathbf{mod}\ n .$$

said exponent v is such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of the base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

the two equations:

$$x^2 \equiv g_i \mathbf{mod}\ n \text{ and } x^2 \equiv -g_i \mathbf{mod}\ n$$

cannot be resolved in x in the ring of integers modulo n

and such that:

the equation:

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

can be resolved in x in the ring of the integers modulo n;

said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

the witness device comprises

- a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or $f.m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) of the private values Q_i and of the public exponent v ;

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments $\mathbb{R}$ of the witness device, to compute commitments $\mathbb{R}$ in the ring of integers modulo n; each commitment being computed:

◦ either by performing operations of the type:

$$\mathbb{R} \equiv r^v \bmod n$$

where r is a random value produced by the random value production means, r being such that $0 < r < n$,

◦ or by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses $\mathbb{D}$ of the witness device for the computation, on the basis of each challenge d, of a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method.

- transmission means to transmit one or more commitments $\mathbb{R}$ and one or more responses $\mathbb{D}$;

there are as many responses $\mathbb{D}$ as there are challenges d as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, d, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

7. A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

◦ **Step 1: act of commitment R**

at each call, the means of computation of the commitments R of the witness device compute each commitment R by applying the process specified according to claim 1,

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment R to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment R to the controller device through the connection means;

◦ **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment R, of the challenges **d** equal in number to the number of commitments R,

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means ;

◦ **Step 3: act of response $\mathbb{D}$**

the means of reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the demonstrator device through the interconnection means,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbf{d}$ by applying the process specified according to claim 1,

◦ **Step 4: act of checking**

the transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment $\mathbb{R}$.

if the transmission means of the demonstrator have transmitted a part of each commitment $\mathbb{R}$, the computation means of the controller device, having $\mathbf{m}$ public values G_1, G_2, ..., G_m, compute a reconstructed commitment $\mathbb{R}'$, from each challenge $\mathbf{d}$ and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

the comparison means of the controller device compare each reconstructed commitment $\mathbb{R}'$ with all or part of each commitment $\mathbb{R}$ received,

case where the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

if the transmission means of the demonstrator have transmitted the totality of each commitment $\mathbb{R}$, the computation means and the comparison means of the controller

device, having **m** public values $G_1, G_2, ..., G_m$, ascertain that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

8. System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified in claim 1

the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

◦ **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose

arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token $\mathbb{T}$ through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token $\mathbb{T}$, of the challenges $\mathbf{d}$ in a number equal to the number of commitments $\mathbb{R}$,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges $\mathbf{d}$ to the demonstrator through the connection means;

- **Step 3: act of response $\mathbb{D}$**

the means of reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the demonstrator device through the interconnection means,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbf{d}$ by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having $\mathbf{m}$ public values $G_1, G_2, ..., G_m$, to firstly compute a reconstructed commitment $\mathbb{R}'$, from each challenge $\mathbf{d}$ and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

then, secondly, compute a token $\mathbb{T}'$ by applying the hashing function $\mathbf{h}$ having as arguments the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token $\mathbb{T}'$ with the received token $\mathbb{T}$.

9. System according to claim 6, designed to produce the digital signature of a message $\mathbb{M}$, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message $\mathbb{M}$,
- the challenges $\mathbf{d}$ and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

◦ **Step 2: act of challenge $\mathbf{d}$**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function $\mathbf{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute a binary train and extract, from this binary train, challenges $\mathbf{d}$ whose number is equal to the number of commitments $\mathbb{R}$,

◦ **Step 3: act of response $\mathbb{D}$**

the means for the reception of the challenges $\mathbb{d}$ of the witness device receive each challenge $\mathbb{d}$ coming from the signing device through the interconnection means,

the means for computing the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbb{d}$ by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbb{D}$ to the signing device through the interconnection means.

10. System according to claim 9, designed to prove the authenticity of the message $\mathbb{M}$ by checking the signed message by means of an entity called the controller;

Checking operation

the system being such that it comprises a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;

the signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message $\mathbb{M}$,
- the challenges $\mathbb{d}$ and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device,

◦ **case where the controller device has commitments $\mathbb{R}$, challenges $\mathbb{d}$, responses $\mathbb{D}$**

if the controller has commitments $\mathbb{R}$, challenges $\mathbf{d}$, responses $\mathbb{D}$,

◦ ◦ the computation and comparison means of the controller device ascertain that the commitments $\mathbb{R}$, the challenges $\mathbf{d}$ and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

◦ ◦ the computation and comparison means of the controller device ascertain that the message $\mathbb{M}$, the challenges $\mathbf{d}$ and the commitments $\mathbb{R}$ satisfy the hashing function:

$$\mathbf{d} = \mathbf{h}\ (\text{message}, \mathbb{R})$$

◦ **case where the controller device has challenges $\mathbf{d}$ and responses $\mathbb{D}$**

if the controller device has challenges $\mathbf{d}$ and responses $\mathbb{D}$,

◦ ◦ the computation means of the controller, on the basis of each challenge $\mathbf{d}$ and each response $\mathbb{D}$, compute commitments $\mathbb{R}'$ satisfying relationships of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

◦ ◦ the computation and comparison means of the controller device ascertain that the message $\mathbb{M}$ and the challenges $\mathbf{d}$ satisfy the hashing function:

$$\mathbf{d} = \mathbf{h}\ (\text{message}, \mathbb{R}')$$

◦ **case where the controller device has commitments $\mathbb{R}$ and responses $\mathbb{D}$**

if the controller device has commitments $\mathbb{R}$ and responses $\mathbb{D}$,

◦ ◦ the computation means of the controller device apply the hashing function and compute $\mathbf{d}'$ such that

$$\mathbf{d}' = \mathbf{h}\ (\text{message}, \mathbb{R})$$

◦ ◦ the computation and comparison means of the controller device ascertain that the commitments $\mathbb{R}$, the challenges $\mathbf{d}'$ and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^{v}/G_1^{\,d'1} \,.\, G_2^{\,d'2} \,.\, \ldots\, G_m^{\,d'm} \,.\, \mathbf{mod}\ n$$

11. A terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity;

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (m being greater than or equal to 1),
- a public modulus n constituted by the product of said f prime factors $p_1, p_2, \ldots p_f$ (f being greater than or equal to 2),
- a public exponent v.

said modulus, said exponent and said values being related by relations of the type

$$G_i \,.\, Q_i^{\,v} \equiv 1 \,.\, \mathbf{mod}\ n \text{ or } G_i \equiv Q_i^{\,v}\ \mathbf{mod}\ n \,.$$

said exponent v being such that

$$v = 2^k$$

where k is a security parameter greater than 1.

said public value G_i being the square g_i^2 of the base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

the two equations:

$$x^2 \equiv g_i\ \mathbf{mod}\ n \quad \text{and} \quad x^2 \equiv -\,g_i\ \mathbf{mod}\ n$$

cannot be resolved in x in the ring of integers modulo n

and such that

the equation:

$$x^v \equiv g_i^2\ \mathbf{mod}\ n$$

can be resolved in x in the ring of the integers modulo n.

said terminal device comprises a witness device comprising,

- a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or $f.m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v.

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments $\mathbb{R}$ of the witness device, to compute commitments $\mathbb{R}$ in the ring of the integers modulo n; each commitment being computed:

◦ either by performing operations of the type:

$$\mathbb{R} \equiv r^v \bmod n$$

where r is a random value produced by the random value production means, r being such that $0 < r < n$,

◦ or by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$ produced by the random value production means, then by applying the Chinese remainder method;

the witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses $\mathbb{D}$ of the witness device, for the computation, on the basis of each challenge d, of a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method,

- transmission means to transmit one or more commitments $\mathbb{R}$ and one or more responses $\mathbb{D}$;

there are as many responses $\mathbb{D}$ as there are challenges d as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, d, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

12. A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1, the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment $\mathbb{R}$ to the controller device, through the connection means;

◦ **Steps 2 and 3: act of challenge d, act of response $\mathbb{D}$**

the means of reception of the challenges d of the witness device receive each challenge d coming from the controller device through the connection means

between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller that carries out the check.

13. Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1;

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

- **Steps 2 and 3: act of challenge d, act of response $\mathbb{D}$**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token $\mathbb{T}$, through the connection means, to the controller device,

*(said controller, after having received the token **T**, produces challenges **d** in a number equal to the number of commitments **R**,)*

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator send each response $\mathbb{D}$ to the controller device which performs the check.

14. Terminal device according to claim 11, designed to produce the digital signature of a message $\mathbb{M}$, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits

in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the signing device through the interconnection means,

- **Step 2: act of challenge $\mathbf{d}$**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function $\mathbf{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute a binary train and extract, from this binary train, challenges $\mathbf{d}$ whose number is equal to the number of commitments $\mathbb{R}$,

- **Step 3: act of response $\mathbb{D}$**

the means for the reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the signing device through the interconnection means,

the means for computing the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbf{d}$ by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbb{D}$ to the signing device, through the interconnection means.

15. Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to check:

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity

by means of all or part of the following parameters or derivatives of these parameters:

- $\mathbb{m}$ pairs of public values $\mathbb{G}_1, \mathbb{G}_2, \ldots \mathbb{G}_m$ ($\mathbb{m}$ being greater than or equal to 1),
- a public modulus $\mathbb{n}$ constituted by the product of said $\mathbb{f}$ prime factors $\mathbb{p}_1, \mathbb{p}_2, \ldots \mathbb{p}_f$ ($\mathbb{f}$ being greater than or equal to 2), unknown to the controller device and to the associated controller entity,
- a public exponent v;

said modulus, said exponent and said values being related by relations of the type

$$\mathbb{G}_i \cdot \mathbb{Q}_i^{\mathbb{v}} \equiv 1 \ . \bmod \mathbb{n} \text{ or } \mathbb{G}_i \equiv \mathbb{Q}_i^{\mathbb{v}} \bmod \mathbb{n} \ .$$

where $\mathbb{Q}_i$ designates a private value, unknown to the controller device, associated with the public value $\mathbb{G}_i$.

said exponent v being such that

$$\mathbb{v} = 2^{\mathbb{k}}$$

where $\mathbb{k}$ is a security parameter greater than 1;

said public value $\mathbb{G}_i$ being the square $\mathbb{g}_i^2$ of a base number $\mathbb{g}_i$ smaller than the $\mathbb{f}$ prime factors $\mathbb{p}_1, \mathbb{p}_2, \ldots \mathbb{p}_f$, the base number $\mathbb{g}_i$ being such that

the two equations:

$$\mathbb{x}^2 \equiv \mathbb{g}_i \bmod \mathbb{n} \text{ and } \mathbb{x}^2 \equiv - \mathbb{g}_i \bmod \mathbb{n}$$

cannot be resolved in x in the ring of integers modulo $\mathbb{n}$ and such that:

the equation:

$$\mathbb{x}^{\mathbb{v}} \equiv \mathbb{g}_i^2 \bmod \mathbb{n}$$

can be resolved in x in the ring of the integers modulo $\mathbb{n}$.

16. Controller device according to claim 15, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing

communications network, to a demonstrator device associated with the demonstrator entity;

sid controller device being used to execute the following steps:

◦ **Steps 1 and 2: act of commitment $\mathbb{R}$, act of challenge d**

said controller device also has means for the reception of all or part of the commitments $\mathbb{R}$ coming from the demonstrator device through the connection means, the controller device has challenge production means for the production, after receiving all or part of each commitment $\mathbb{R}$, of the challenges **d** in a number equal to the number of commitments $\mathbb{R}$, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges.

the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

◦ **Steps 3 and 4: act of response $\mathbb{D}$, act of checking**

said controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,
- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment $\mathbb{R}$.

if the reception means of the demonstrator have received a part of each commitment $\mathbb{R}$, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

the comparison means of the controller device compare each reconstructed commitment $\mathbb{R}'$ with all or part of each commitment $\mathbb{R}$ received,

case where the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

if the transmission means of the demonstrator have received the totality of each commitment $\mathbb{R}$, the computation means and the comparison means of the controller device, having m public values $G_1, G_2, ..., G_m$, ascertain that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

17. Controller device according to claim 15, designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity known as a demonstrator,

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity,

said system enabling the execution of the following steps:

- **Steps 1 and 2: act of commitment $\mathbb{R}$, act of challenge d**

said controller device also has means for the reception of tokens $\mathbb{T}$ coming from the demonstrator device through the connection means,

the controller device has challenge production means for the production, after having received the token $\mathbb{T}$, of the challenges d in a number equal to the number of commitments $\mathbb{R}$, each challenge d comprising m integers d_i, herein after called elementary challenges,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means;

- **Steps 3 and 4: act of response $\mathbb{D}$, act of checking**

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device;

◦ **case where the controller device has commitments $\mathbb{R}$, challenges d, responses $\mathbb{D}$**

if the controller has commitments $\mathbb{R}$, challenges **d**, responses $\mathbb{D}$,

◦ ◦ the computation and comparison means of the controller device ascertain that the commitments $\mathbb{R}$, the challenges **d** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

◦ ◦ the computation and comparison means of the controller device ascertain that the message $\mathbb{M}$, the challenges **d** and the commitments $\mathbb{R}$ satisfy the hashing function

$$d = h(\text{message}, \mathbb{R})$$

◦ **case where the controller device has challenges d and responses $\mathbb{D}$**

if the controller device has challenges **d** and responses $\mathbb{D}$,

◦ ◦ the computation means of the controller, on the basis of each challenge **d** and each response $\mathbb{D}$, compute commitments $\mathbb{R}'$ satisfying relationships of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R}' \equiv \mathbb{D}^v/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

◦ ◦ the computation and comparison means of the controller device ascertain that the message $\mathbb{M}$ and the challenges **d** satisfy the hashing function:

$$d = h(\text{message}, \mathbb{R}')$$

◦ **case where the controller device has commitments $\mathbb{R}$ and responses $\mathbb{D}$**

if the controller device has commitments $\mathbb{R}$ and responses $\mathbb{D}$,

◦ ◦ the computation means of the controller device apply the hashing function and compute **d'** such that

$$d' = h \text{ (message, R)}$$

• • the computation and comparison means of the controller device ascertain that the commitments **R,** the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v/G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/32

A2

(11) Numéro de publication internationale: WO 00/45550

(43) Date de publication internationale: 3 août 2000 (03.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00190

(22) Date de dépôt international: 27 janvier 2000 (27.01.00)

(30) Données relatives à la priorité:

99/01065	27 janvier 1999 (27.01.99)	FR
99/03770	23 mars 1999 (23.03.99)	FR
99/12465	1er octobre 1999 (01.10.99)	FR
99/12467	1er octobre 1999 (01.10.99)	FR
99/12468	1er octobre 1999 (01.10.99)	FR

(71) Déposants *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F–75015 Paris (FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour–sur–Glane, F–75732 Paris cedex 15 (FR). MATH RIZK [BE/BE]; Verte Voie, 20 Boîte 5, B–1348 Louvain–la–Neuve (BE).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(US seulement)*: GUILLOU, Louis [FR/FR]; 16, rue de l'Ise, F–35230 Bourgbarre (FR). QUISQUATER, Jean–Jacques [BE/BE]; 3, avenue des Canards, B–1640 Rhode Saint Genese (BE).

(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F–35700 Rennes (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.

(54) Title: METHOD FOR PROVING THE AUTHENTICITY OR INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC EXPONENT EQUAL TO THE POWER OF TWO

(54) Titre: PROCEDE DESTINE A PROUVER L'AUTHENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN MESSAGE AU MOYEN D'UN EXPOSANT PUBLIC EGAL A UNE PUISSANCE DE DEUX

(57) Abstract

Proof is established by means of the following parameters: m pairs of private values Q_i and public values G_i, m>1, a public module n made of the product of f first factors p_j, f>2, a public exponent v, linked to each other by relations of the type: $G_i.Q_i^v = 1 \bmod n$ or $G_i=Q_i^v \bmod n$. Said exponent v is such that $v=2^k$ where k>1 is a security parameter. Public value G_i is the square g_i^2 of a base number g_i that is lower than f first factors p_j, so that the two equations: $x2=g_i \bmod n$ and $x^2=-g_i \bmod n$ do not have a solution in x in the ring of the modulo n integers and such that the equation $x^v=g_i^2 \bmod n$ has solutions in x in the ring of the modulus n integers.

(57) Abrégé

La preuve est établie au moyen des paramètres suivants: m couples de valeurs privées Q_i et publiques G_i, m>1; un module public n constitué par le produit de f facteurs premiers p_j, f>2, un exposant public v, liés par des relations du type: $G_i.Q_i^v = 1 \bmod n$ ou $G_i=Q_i^v \bmod n$. Ledit exposant v est tel que $v = 2^k$ où k>1 est un paramètre de sécurité. Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_j, tel que les deux équations: $x^2 = g_i \bmod n$ et $x^2 = -g_i \bmod n$ n'ont pas de solution en x dans l'anneau des entiers modulo n, et tel que l'équation $x^v = g_i^2 \bmod n$ a des solutions en x dans l'anneau des entiers modulo n.

09/889,918

TEXT AS AMENDED

CLAIMS

1. Method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n;

said method implements, in the following steps, an entity called a witness having f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments $\mathbb{R}$ in the ring of the integers modulo n; each commitment being computed:

◦ either by performing operations of the type:

$$\mathbb{R} \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

◦ or

◦ ◦ by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

◦ ◦ then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or

◦ ◦ by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

◦ ◦ and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbb{D}$ as there are challenges d as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, d, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

2. Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

- at each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified in claim 1,

- the demonstrator sends the controller all or part of each commitment $\mathbb{R}$,

◦ **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment $\mathbb{R}$, produces challenges **d** whose number is equal to the number of commitments $\mathbb{R}$ and sends the challenges **d** to the demonstrator,

◦ **Step 3: act of response $\mathbb{D}$**

- the witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the process specified in claim 1,

◦ **Step 4: act of checking**

- the demonstrator sends each response $\mathbb{D}$ to the controller,

case where the demonstrator has transmitted a part of each commitment $\mathbb{R}$

if the demonstrator has transmitted a part of each commitment $\mathbb{R}$, the controller, having the **m** public values $G_1, G_2, ..., G_m$, computes a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

the controller ascertains that each reconstructed commitment $\mathbb{R}'$ reproduces all or part of each commitment $\mathbb{R}$ that has been transmitted to it.

case where the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

if the demonstrator has transmitted the totality of each commitment $\mathbb{R}$, the controller, having the **m** public values $G_1, G_2, ..., G_m$, ascertains that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

3. Method according to claim 1, designed to provide proof to an entity, known as the controller entity, of the integrity of a message $\mathbb{M}$ associated with an entity called a demonstrator entity, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

◦ **Step 1: act of commitment R**

- at each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

◦ **Step 2: act of challenge d**

- the demonstrator applies a hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$,
- the demonstrator sends the token $\mathbb{T}$ to the controller,
- the controller, after having received a token $\mathbb{T}$, produces challenges **d** equal in number to the number of commitments $\mathbb{R}$ and sends the challenges **d** to the demonstrator,

◦ **Step 3: act of response $\mathbb{D}$**

- the witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

◦ **Step 4: act of checking**

- the demonstrator sends each response $\mathbb{D}$ to the controller,
- the controller, having the **m** public values $\mathbb{G}_1$, $\mathbb{G}_2$, ..., $\mathbb{G}_m$, computes a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv \mathbb{G}_1^{\,d1} \cdot \mathbb{G}_2^{\,d2} \cdot \ldots \mathbb{G}_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v/\mathbb{G}_1^{\,d1} \cdot \mathbb{G}_2^{\,d2} \cdot \ldots \mathbb{G}_m^{\,dm} \cdot \bmod n$$

- then the controller applies the hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$ to reconstruct the token $\mathbb{T}'$,
- then the controller ascertains that the token $\mathbb{T}'$ is identical to the token $\mathbb{T}$ transmitted.

4. Method according to claim 1, designed to produce the digital signature of a message $\mathbb{M}$ by an entity known as the signing entity, said signing entity comprising the witness;

Signing operation

said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

said signing entity executes the signing operation by implementing the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

- at each call, the witness computes each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

◦ **Step 2: act of challenge d**

- the signing party applies a hashing function **h** whose arguments are the message $\mathbb{M}$ and each commitment $\mathbb{R}$ to obtain a binary train,
- from this binary train, the signing party extracts challenges **d** whose number is equal to the number of commitments $\mathbb{R}$,

◦ **Step 3: act of response $\mathbb{D}$**

- the witness computes the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1.

5. Method according to claim 4, designed to prove the authenticity of the message M by checking the signed message through an entity called a controller;

Checking operation

- said controller entity having the signed message executes a checking operation by proceeding as follows:

◦ **case where the controller has commitments $\mathbb{R}$, challenges d, responses $\mathbb{D}$**

if the controller has commitments $\mathbb{R}$, challenges **d**, responses $\mathbb{D}$,

◦ ◦ the controller ascertains that the commitments $\mathbb{R}$, the challenges **d** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

◦ ◦ the controller ascertains that the message $\mathbb{M}$, the challenges **d** and the commitments $\mathbb{R}$ satisfy the hashing function:

$$\mathbf{d = h\ (message, \mathbb{R})}$$

◦ **case where the controller has challenges d and responses $\mathbb{D}$**

if the controller has challenges **d** and responses $\mathbb{D}$,

◦ ◦ the controller reconstructs, on the basis of each challenge **d** and each response $\mathbb{D}$, commitments $\mathbb{R}'$ satisfying relationships of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

◦ ◦ the controller ascertains that the message $\mathbb{M}$ and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, \mathbb{R}')}$$

◦ **case where the controller has commitments $\mathbb{R}$ and responses $\mathbb{D}$**

if the controller has commitments $\mathbb{R}$ and responses $\mathbb{D}$,

◦ ◦ the controller applies the hashing function and reconstructs **d'**

$$\mathbf{d' = h\ (message, \mathbb{R})}$$

◦ ◦ the controller device ascertains that the commitments $\mathbb{R}$, the challenges **d'** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

6. A system designed to prove, to a controller server,

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity,

by means of:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or parameters derived from these values,
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2,

said modulus and said values being linked by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \cdot \mathbf{mod}\ n \text{ or } G_i \equiv Q_i^v \mathbf{mod}\ n .$$

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of the base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that the following conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \mathbf{mod}\ n \text{ and } x^2 \equiv -g_i \mathbf{mod}\ n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \mathbf{mod}\ n$$

can be resolved in x in the ring of the integers modulo n;

said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

the witness device comprises

- a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \mathbf{mod}\ p_j$) of the private values Q_i and of the public exponent v;

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of integers modulo n; each commitment being computed:

  - either by performing operations of the type:

$$R \equiv r^v \mathbf{mod}\ n$$

where r is a random value produced by the random value production means, r being

such that $0 < r < n$,

◦ or by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses $\mathbb{D}$ of the witness device for the computation, on the basis of each challenge **d, of** a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method.

- transmission means to transmit one or more commitments $\mathbb{R}$ and one or more responses $\mathbb{D}$;

there are as many responses $\mathbb{D}$ as there are challenges **d** as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, **d**, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, d, \mathbb{D}\}$.

7. A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment $\mathbb{R}$ to the controller device through the connection means;

- **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment $\mathbb{R}$, of the challenges **d** equal in number to the number of commitments $\mathbb{R}$,

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

- **Step 3: act of response $\mathbb{D}$**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment $\mathbb{R}$.

if the transmission means of the demonstrator have transmitted a part of each commitment $\mathbb{R}$, the computation means of the controller device, having **m** public values G_1, G_2, ..., G_m, compute a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

the comparison means of the controller device compare each reconstructed commitment $\mathbb{R}'$ with all or part of each commitment $\mathbb{R}$ received,

case where the demonstrator has transmitted the totality of each commitment $\mathbb{R}$

if the transmission means of the demonstrator have transmitted the totality of each commitment $\mathbb{R}$, the computation means and the comparison means of the controller device, having **m** public values G_1, G_2, ..., G_m, ascertain that each commitment $\mathbb{R}$ satisfies a relationship of the type

$$\mathbb{R} \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

8. System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified in claim 1

the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

◦ **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function $\mathbb{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token $\mathbb{T}$ through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token $\mathbb{T}$, of the challenges $\mathbf{d}$ in a number equal to the number of commitments $\mathbb{R}$,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

- **Step 3: act of response $\mathbb{D}$**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $G_1, G_2, ..., G_m$, to firstly compute a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

then, secondly, compute a token $\mathbb{T}'$ by applying the hashing function h having as arguments the message $\mathbb{M}$ and all or part of each reconstructed commitment $\mathbb{R}'$,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token $\mathbb{T}'$ with the received token $\mathbb{T}$.

9. System according to claim 6, designed to produce the digital signature of a message $\mathbb{M}$, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message $\mathbb{M}$,

- the challenges $\mathbf{d}$ and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

- **Step 2: act of challenge $\mathbf{d}$**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function $\mathbf{h}$ whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute a binary train and extract, from this binary train, challenges $\mathbf{d}$ whose number is equal to the number of commitments $\mathbb{R}$,

- **Step 3: act of response $\mathbb{D}$**

the means for the reception of the challenges $\mathbf{d}$ of the witness device receive each challenge $\mathbf{d}$ coming from the signing device through the interconnection means,

the means for computing the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges $\mathbf{d}$ by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbb{D}$ to the signing device through the interconnection means.

10. System according to claim 9, designed to prove the authenticity of the message $\mathbb{M}$ by checking the signed message by means of an entity called the controller;

Checking operation

the system being such that it comprises a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;

the signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

∘ case where the controller device has commitments $\mathbb{R}$, challenges d, responses $\mathbb{D}$

if the controller has commitments $\mathbb{R}$, challenges **d**, responses $\mathbb{D}$,

∘ ∘ the computation and comparison means of the controller device ascertain that the commitments $\mathbb{R}$, the challenges **d** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

◦ ◦ the computation and comparison means of the controller device ascertain that the message $\mathbb{M}$, the challenges **d** and the commitments $\mathbb{R}$ satisfy the hashing function:

$$\mathbf{d = h\ (message, \mathbb{R})}$$

◦ **case where the controller device has challenges d and responses $\mathbb{D}$**

if the controller device has challenges **d** and responses $\mathbb{D}$,

◦ ◦ the computation means of the controller, on the basis of each challenge **d** and each response $\mathbb{D}$, compute commitments $\mathbb{R}$' satisfying relationships of the type

$$\mathbb{R}' \equiv G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{\,d1} \cdot G_2^{\,d2} \cdot \ldots G_m^{\,dm} \cdot \bmod n$$

◦ ◦ the computation and comparison means of the controller device ascertain that the message $\mathbb{M}$ and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, \mathbb{R}')}$$

◦ **case where the controller device has commitments $\mathbb{R}$ and responses $\mathbb{D}$**

if the controller device has commitments $\mathbb{R}$ and responses $\mathbb{D}$,

◦ ◦ the computation means of the controller device apply the hashing function and compute **d'** such that

$$\mathbf{d' = h\ (message, \mathbb{R})}$$

◦ ◦ the computation and comparison means of the controller device ascertain that the commitments $\mathbb{R}$, the challenges **d'** and the responses $\mathbb{D}$ satisfy relationships of the type

$$\mathbb{R} \equiv G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \mathbb{D}^v \bmod n$$

or relationships of the type:

$$\mathbb{R} \equiv \mathbb{D}^v / G_1^{\,d'1} \cdot G_2^{\,d'2} \cdot \ldots G_m^{\,d'm} \cdot \bmod n$$

11. A terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity;

by means of :

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or parameters derived from these values,

- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),

said modulus and said values being related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \bmod n \text{ or } G_i \equiv Q_i^{-v} \bmod n .$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

said public value G_i being the square g_i^2 of the base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**.

said terminal device comprises a witness device comprising,

- a memory zone containing the **f** prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v**.

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device, to compute commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

  - either by performing operations of the type:

$$\mathbb{R} \equiv r^{v} \bmod n$$

where r is a random value produced by the random value production means, r being such that $0 < r < n$,

◦ or by performing operations of the type:

$$\mathbb{R}_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$ produced by the random value production means, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses $\mathbb{D}$ of the witness device, for the computation, on the basis of each challenge **d**, of a response $\mathbb{D}$,

◦ either by performing operations of the type:

$$\mathbb{D} \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

◦ or by performing operations of the type:

$$\mathbb{D}_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainder method,

- transmission means to transmit one or more commitments $\mathbb{R}$ and one or more responses $\mathbb{D}$;

there are as many responses $\mathbb{D}$ as there are challenges **d** as there are commitments $\mathbb{R}$, each group of numbers $\mathbb{R}$, **d**, $\mathbb{D}$ forming a triplet referenced $\{\mathbb{R}, \mathbf{d}, \mathbb{D}\}$.

12. A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the

form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1,

the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment $\mathbb{R}$ to the controller device, through the connection means;

- **Steps 2 and 3: act of challenge d, act of response $\mathbb{D}$**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response $\mathbb{D}$ to the controller that carries out the check.

13. Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message $\mathbb{M}$ associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

- **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1;

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the demonstrator device through the interconnection means,

- **Steps 2 and 3: act of challenge d, act of response $\mathbb{D}$**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function h whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute at least one token $\mathbb{T}$,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token $\mathbb{T}$, through the connection means, to the controller device,

said controller, after having received the token $\mathbb{T}$, produces challenges d equal in number to the number of commitments $\mathbb{R}$,

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

◦ **Step 4: act of checking**

the transmission means of the demonstrator send each response $\mathbb{D}$ to the controller device which performs the check.

14. Terminal device according to claim 11, designed to produce the digital signature of a message $\mathbb{M}$, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message $\mathbb{M}$,
- the challenges **d** and/or the commitments $\mathbb{R}$,
- the responses $\mathbb{D}$;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

◦ **Step 1: act of commitment $\mathbb{R}$**

at each call, the means of computation of the commitments $\mathbb{R}$ of the witness device compute each commitment $\mathbb{R}$ by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbb{R}$ to the signing device through the interconnection means,

- **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message $\mathbb{M}$ and all or part of each commitment $\mathbb{R}$ to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments $\mathbb{R}$,

- **Step 3: act of response $\mathbb{D}$**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses $\mathbb{D}$ of the witness device compute the responses $\mathbb{D}$ from the challenges **d** by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbb{D}$ to the signing device, through the interconnection means.

15. Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to check:

- the authenticity of an entity and/or
- the integrity of a message $\mathbb{M}$ associated with this entity

by means of:

- **m** pairs of public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1,
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2, unknown to the controller device and to the associated controller entity,

said modulus and said values being related by relations of the type

$$\mathbb{G}_i \cdot \mathbb{Q}_i^{v} \equiv 1 \ . \ \mathbf{mod\ n} \text{ or } \mathbb{G}_i \equiv \mathbb{Q}_i^{v} \ \mathbf{mod\ n} \ .$$

where $\mathbb{Q}_i$ designates a private value, unknown to the controller device, associated with the public value $\mathbb{G}_i$.

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value $\mathbb{G}_i$ being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that the following conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \ \mathbf{mod\ n} \quad \text{and} \quad x^2 \equiv -\, g_i \ \mathbf{mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \ \mathbf{mod\ n}$$

can be resolved in x in the ring of the integers modulo **n.**

16. Controller device according to claim 15, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity;

sid controller device being used to execute the following steps:

- **Steps 1 and 2: act of commitment $\mathbb{R}$, act of challenge d**

said controller device also has means for the reception of all or part of the commitments $\mathbb{R}$ coming from the demonstrator device through the connection means, the controller device has challenge production means for the production, after receiving all or part of each commitment $\mathbb{R}$, of the challenges **d** in a number equal to the number of commitments $\mathbb{R}$, each challenge **d** comprising **m** integers d_j hereinafter called elementary challenges.

the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

◦ **Steps 3 and 4: act of response $\mathbb{D}$, act of checking**

said controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment $\mathbb{R}$.

if the reception means of the demonstrator have received a part of each commitment $\mathbb{R}$, the computation means of the controller device, having **m** public values G_1, G_2, ..., G_m, compute a reconstructed commitment $\mathbb{R}'$, from each challenge **d** and each response $\mathbb{D}$, this reconstructed commitment $\mathbb{R}'$ satisfying a relationship of the type

$$\mathbb{R}' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathbb{D}^v \bmod n$$

or a relationship of the type

$$\mathbb{R}' \equiv \mathbb{D}^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

the comparison means of the controller device compare each reconstructed commitment $\mathbb{R}'$ with all or part of each commitment $\mathbb{R}$ received,